

大容量语音教学视频
直观引导配置操作

网管天下

网络安全

陈忠平 李旋 刘青凤 等编著

理论深刻透彻
配置直观明了

清华大学出版社

网 络 安 全

陈忠平　李　旎　刘青凤　等编著

清 华 大 学 出 版 社
北　京

内 容 简 介

本书介绍网络安全方面的知识，具体包括认识网络安全、网络操作系统安全、网络设备安全、防火墙安全体系、加密技术及备份技术等。本书还插入大量的网络工具列表内容，让用户充分了解用于保证网络安全所需的各种关键技术和工具的应用等。

本书适用于中小企业网络管理人员、企业 IT 经理和网络管理员以及网络安全工程师自学选用，也可作为高校的选用教材和参考手册。

图书在版编目（CIP）数据

网络安全 / 陈忠平等编著. —北京：清华大学出版社，2011.1
ISBN 978-7-302-24365-6

Ⅰ. ①网…　Ⅱ. ①陈…　Ⅲ. ①计算机网络 – 安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 257902 号

责任编辑：夏兆彦
责任校对：徐俊伟
责任印制：
出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：190×260　**印　张：**27.25　**插　页：**2　**字　数：**677 千字
版　次：2011 年 1 月第 1 版　**印　次：**2011 年 1 月第 1 次印刷
印　数：1～ 000
定　价：　元

产品编号：031003-01

FOREWORD

前言

网络已成为主要的数据传输和信息交换平台，许多部门和企业在网上构建了关键的业务流程。网络安全和信息安全是保障网上业务正常运行的关键，并已日益成为网络用户普遍关注的焦点问题。

本书介绍网络安全方面的知识，具体包括认识网络安全、网络操作系统安全、网络设备安全、防火墙安全体系、加密技术及备份技术等。本书还插入大量的网络工具列表内容，让用户充分了解用于保证网络安全所需的各种关键技术和工具的应用等。

1. 本书内容

本书分篇介绍与网络安全相关的重点内容，语言简单易懂、内容深入浅出，并插入大量的实例案例图形，使用户能更好地掌握该方面的技术。

本书共分 5 篇 13 章。

第一篇为认识网络安全（包含第 1～3 章），介绍网络安全的基础内容，使用户拥有扎实的理论知识。

第 1 章为网络安全基础，详细介绍网络安全概念、网络安全评价标准、常见的安全威胁与攻击、网络安全的现状和发展趋势等。

第 2 章为计算病毒，详细介绍计算机病毒概述、计算机病毒的危害、常见的计算机病毒类型、网络工具列表等。

第 3 章为网络攻击与防范，详细介绍黑客概述、常见的网络攻击、木马攻击与分析、木马的攻击防护技术等。

第二篇为网络操作系统安全（包含第 4～6 章），介绍 Windows Server 2008 服务器操作系统中的安全应用等。

第 4 章为操作系统加固，详细介绍操作系统安装与更新、Internet 连接防火墙、安全配置向导、默认共享等。

第 5 章为系统安全策略，详细介绍账户策略、审核策略、限制用户登录、安全配置和分析、IPSec 安全策略等。

第 6 章为系统漏洞修补，详细介绍漏洞概述、漏洞预警、漏洞更新等。

第三篇为网络设备安全（包含第 7～8 章），典型介绍网络中交换机和路由器的安全配置技术。

第 7 章为交换机安全配置，详细介绍基于端口的传输控制、PVLAN 安全、基于端口的认证安全、配置 RMON 等。

第 8 章为路由器安全配置，详细介绍访问列表安全、网络地址转换、网络攻击安全防范、使用 SDM 配置路由器等。

第四篇为防火墙安全体系（包含第 9～11 章），介绍防火墙基础及

安全设置、Cisco PIX 防火墙的应用、入侵检测系统等。

第 9 章为防火墙基础，则详细介绍防火墙概述、防火墙的分类、防火墙的体系结构、防火墙的主要应用等。

第 10 章为 Cisco PIX 防火墙，详细介绍 PIX 防火墙的概述、PIX 防火墙的基本使用、PIX 防火墙的高级配置、PIX 防火墙系统日志、PIX 防火墙攻击防护等。

第 11 章为入侵检测系统，详细介绍 IDS 的概述、IDS 系统分类、IDS 的检测方式、IDS 的应用、IDS 的发展方向等。

第五篇为加密技术及备份技术（包含第 12、13 章），介绍网络安全中的公钥、数据加密技术和数据备份等。

第 12 章为公钥基础设施，详细介绍 PKI 基础、PKI 服务和实现、PKI 的体系结构、权限管理基础设施 PMI 概况、属性权威和权限管理、基于 PMI 建立安全应用等。

第 13 章为数据加密及备份，详细介绍密钥密码学、数据加密技术、EFS 文件的加密与解密、数据的备份与恢复、数据库的备份与恢复等。

2．本书特色

- 面向职业角度和网管考试安排图书内容，增强了本书的实用性。内容全面，结构完善，形成系统而完备的网管知识体系。
- 通过相关企业征集 30 多个有代表性的、工作中经常应用的一些实例，在书中穿插介绍。将理论知识落实到日常的网络应用实践中，提高读者网络管理的实际应用能力。
- 由具有专业的企业服务器安全管理和网络维护经验的人员编写，对企业环境中面临的安全问题以及解决措施有独特的见解，并能用通俗易懂的语言，深入浅出地表达出来。
- 增加“网管心得”，介绍网管的实际工作环境和职业要求，便于没有工作经验的网管与相关职业接轨，掌握工作中必备技能或者相关知识。

3．读者定位

本书由浅入深，通俗易懂，注重实践，适用于中小企业网络管理人员、企业 IT 经理和网络管理员，以及网络安全工程师自学选用，也可作为高校的选用教材和参考手册。

参与本书编写的除了封面署名人员外，还有胡家宏、王海峰、王健、张勇、冯冠、刘好增、赵俊昌、祁凯、孙江玮、田成军、刘俊杰、王泽波、张银鹤、阎迎利、何方、李海庆、王树兴、朱俊成、康显丽、崔群法、孙岩、秦长海、宋素萍、倪宝童、王立新、温玲娟、于会芳、赵喜来、杨宁宁、郭晓俊、方宁、牛丽萍、郭新志、王黎、安征、亢凤林、李海峰等。由于时间仓促，加之编者水平有限，书中疏漏之处在所难免，欢迎读者朋友登录清华大学出版社的网站 www.tup.com.cn 与我们联系，帮助我们改进提高。

编　者

2010 年 7 月

CONTENTS

目录

第一篇　认识网络安全

第三篇 网络设备安全

第四篇 防火墙安全体系

第五篇 加密技术及备份技术

第一篇　认识网络安全

第1章 网络安全基础

目前，计算机网络的普及度越来越大，不仅是人们工作、学习和生活的便捷工具，同时也为人们提供了各种各样的资源。但是，不得不注意到，网络虽然功能强大，但它有脆弱、易受到攻击的一面。

据美国联绑调查局（FBI）统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。在我国，每年因黑客入侵、计算机病毒对网络的破坏也造成了巨大的经济损失。因此，无论何时网络安全问题不容忽视。

本章从网络安全定义、网络安全概念、常见的安全威胁与攻击、网络安全的现状和发展趋势等方面进行学习，使读者对网络安全有清晰的认识。

本章学习要点：

- 了解网络安全的定义、安全模型及其研究的主要内容
- 熟悉安全的攻防体系结构和层次体系结构
- 了解网络安全评价标准及网络安全自身的脆弱性
- 掌握对网络安全提出的防范建议以及网络所面临的安全威胁种类
- 熟悉网络安全策略设计原则

1.1 网络安全基本概念

随着网络威胁的增加，人们逐渐建立了网络安全研究的相关技术和理论，提出了网络安全的模型、体系结构和目标等。本节从各个方面详细介绍有关网络安全的基础知识。

1.1.1 网络安全概述

网络安全从其本质上来讲就是网络上的信息安全，涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。凡是涉及网络上的信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全所要研究的领域。

严格地说，网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断，这包括如下含义。

- 网络运行系统安全，即保证信息处理和传输系统的安全。
- 网络上系统信息的安全。

- ❑ 网络上信息传播的安全，即信息传播后果的安全。
- ❑ 网络上信息内容的安全，即狭义的“信息安全”。

计算机网络安全的主要内容不仅包括硬件设备、管理控制网络的软件方面，同时也包括共享的资源，快捷的网络服务等方面。具体来讲包括如下内容。

❑ 网络实体安全

计算机机房的物理条件、物理环境及设施的安全，计算机硬件、附属设备及网络传输线路的安装及配置等。

❑ 软件安全

保护网络系统不被非法入侵，系统软件与应用软件不被非法复制、篡改、不受病毒的侵害等。

❑ 数据安全

保护数据不被非法存取，确保其完整性、一致性、机密性等。

❑ 安全管理

在运行期间对突发事件的安全处理，包括采取计算机安全技术，建立安全管理制度，开展安全审计，进行风险分析等内容。

❑ 数据保密性

信息不泄露给非授权的用户、实体或过程，或供其利用的特性。在网络系统的各个层次上有不同的机密性及相应的防范措施。例如，在物理层，要保证系统实体不以电磁的方式（电磁辐射、电磁泄露等）向外泄露信息，在数据处理、传输层面，要保证数据在传输、存储过程中不被非法获取、解析，主要的防范措施是采用密码技术。

❑ 数据完整性

数据完整性指数据在未经授权时不能改变其特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性，完整性要求信息的原样，即信息的正确生成、正确存储和正确传输。影响网络信息完整性的主要因素包括设备故障、传输、处理或存储过程中产生的误码、网络攻击、计算机病毒等，其主要防范措施是校验与认证技术。

❑ 可用性

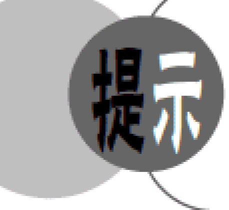
网络信息系统最基本的功能是向用户提供服务，而用户所要求的服务是多层次的、随机的，可用性是指可被授权实体访问，并按需求使用的特性，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

❑ 可控性

可控性指对信息的传播及内容具有控制能力，保障系统依据授权提供服务，使系统任何时候不被非授权用户使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。

❑ 可审查性

提供历史事件的记录，对出现的网络安全问题提供调查的依据和手段。



完整性与保密性不同，保密性要求信息不被泄露给未授权用户，而完整性则是要求信息不受各种原因的破坏。

1.1.2　安全模型

随着信息化社会的网络化，各国的政治、外交、国防等领域越来越依赖于计算机网络，因此，计算机网络安全的地位日趋重要。

从宏观上讲，目前国家、政府部门正在不断制定和完善网络安全的法律、网络安全标准等；而从具体角度讲，针对企业、集团、高校等网络用户而言，拥有经济合理的网络安全设备是保障网络安全的硬件技术，能够协调进行有效的安全管理工作是能够保障网络长期安全、相对稳定运作的动力。而两者所围绕的核心问题是针对预防的主要网络攻击手段及当前运作实体的经济技术能力建立一个可实施的、合理的、长期有效的网络安全模型。

围绕安全模型设计与实施，将相关的网络安全技术与安全机制方面的工作有机结合起来，才能够有效地保证网络安全。所以，建立合理有效的网络安全模型，无论是对硬件设备的选择，还是对后期网络安全管理工作的开展，都是一个关键技术问题。从而也决定了它在实现网络安全方面不可忽视的重要性。网络安全能否有效地担任职责，这对网络技术的发展，网络时代信息秩序的维护以及企业和单位用户的网络正常运行都奠定了坚实的基础。

目前，在网络安全领域存在较多的网络安全模型。这些安全模型都较好地描述了网络安全的部分特征，又都有各自的侧重点，在各自不同的专业和领域都有着一定程度的应用。

1. 基本模型

在网络信息传输中，为了保证信息传输的安全性，一般需要一个值得信任的第三方负责在源节点和目的节点间进行秘密信息分发，同时当双方发生争执时，起到仲裁的作用。

在基本模型中，通信的双方在进行信息传输前，首先建立起一条逻辑通道，并提供安全的机制和服务来实现在开放网络环境中信息的安全传输，图 1-1 为基本安全模型的示意图。

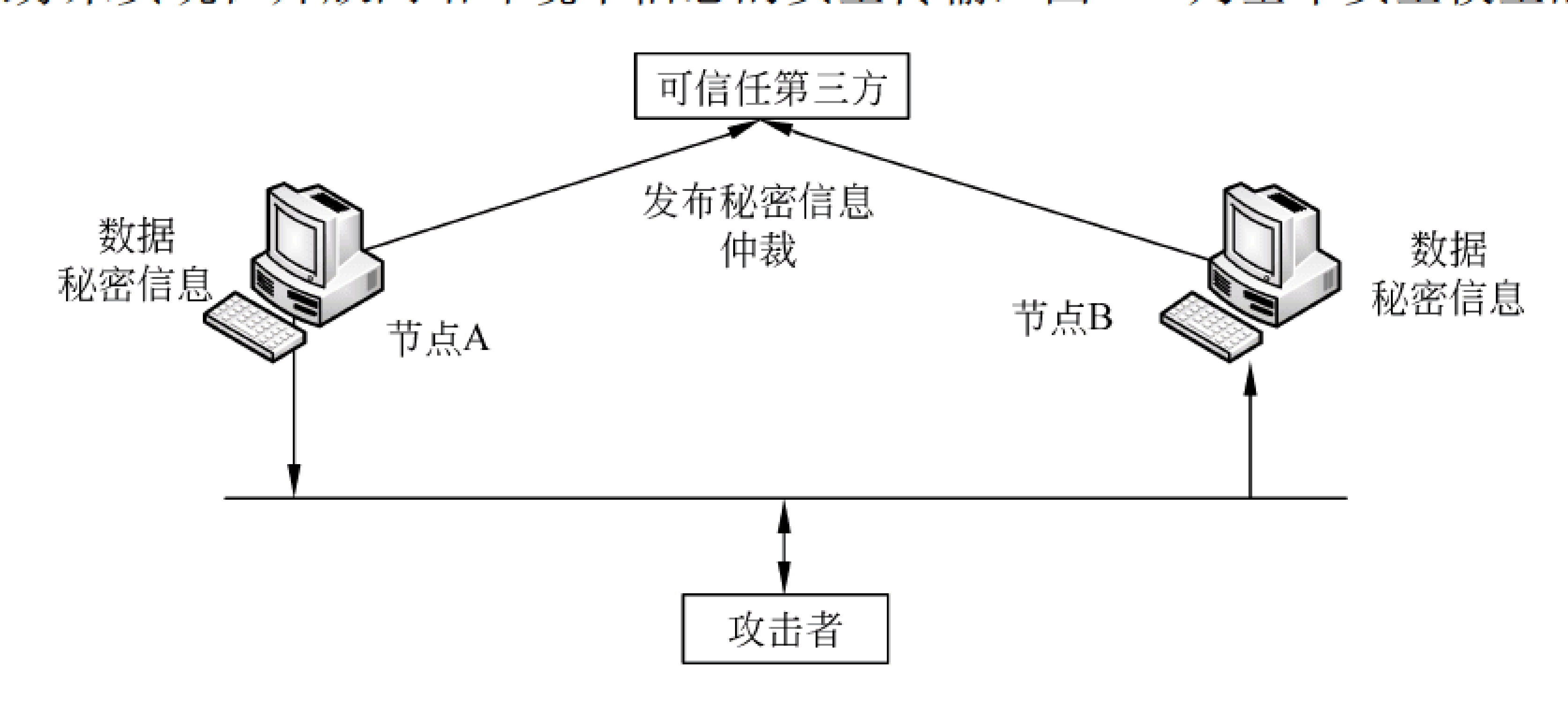


图 1-1　基本安全模型示意图

信息的安全传输主要包括以下两点。

- ❑ 从源节点发出的信息，使用信息加密等加密技术对其进行安全的转发，从而实现该信息的保密性，同时也可以在该信息中附加一些特征信息，作为源节点的身份验证。
- ❑ 源节点与目的节点应该共享如加密密钥这样的保密信息，这些信息除了发送双方和可信任的第三方之外，对其他用户都是保密的。

2. P2DR 模型

P2DR 模型是由美国国际互联网安全系统公司（ISS）提出的动态网络安全理论或称为可适应网络安全理论的主要模型。该模型是美国可信计算机系统评价准则（TCSEC）的发展，也是目前被普遍采用的模型，主要由安全策略（Policy）、防护（Protection）、检测（Detection）和响应（Response）4 部分构成。其中，防护、检测和响应构成了一个所谓完整的、动态的安全循环，在安全策略的整体指导下保证信息系统的安全，图 1-2 为其构成示意图。

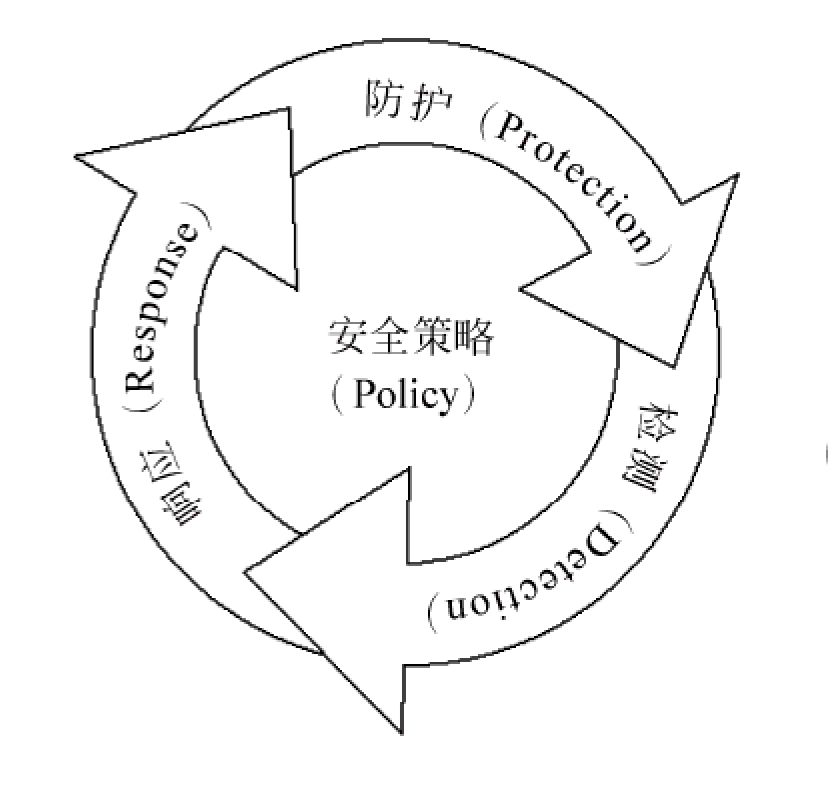


图 1-2　P2DR 模型结构示意图

对于该模型的各组成部分有如下说明。

❑ **安全策略**

安全策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括总体安全策略和具体安全策略两个部分。

❑ **防护**

防护是根据系统可能出现的安全问题而采取的预防措施，这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。

❑ **检测**

当攻击者穿透防护系统时，检测功能就会发挥作用，与防护系统形成互补。检测是动态响应的依据。

❑ **响应**

当系统检测到危及安全的事件、行为、过程时，响应系统就开始工作及对发生事件进行处理，杜绝危害的进一步蔓延扩大，力求系统尚能提供正常服务。响应包括紧急响应和恢复处理两部分，而恢复处理又包括系统恢复和信息恢复。

总之，P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认证、加密等）的同时，利用检测工具（如漏洞评估、入侵检测等）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

1.1.3　网络安全攻防技术

“道高一尺，魔高一丈”，这是网络安全攻击与防御最好的写照。有矛就有盾，也是相互对立的两个方面。而在网络安全中，“攻”和“防”与“矛”和“盾”非常相似。

网络安全的攻防体系结构由网络安全物理基础、网络安全的实施及工具和防御技术三大方面构成，图 1-3 为其结构示意图。

对于用户来讲，如果不知道如何攻击，那么再好的防守也是经不住考验的，目前，常用的攻击技术主要包括 5 个方面。

❑ **网络监听**　自己不主动去攻击别人，在计算机上设置一个程序去监听目标计算机与其

他计算机通信的数据。

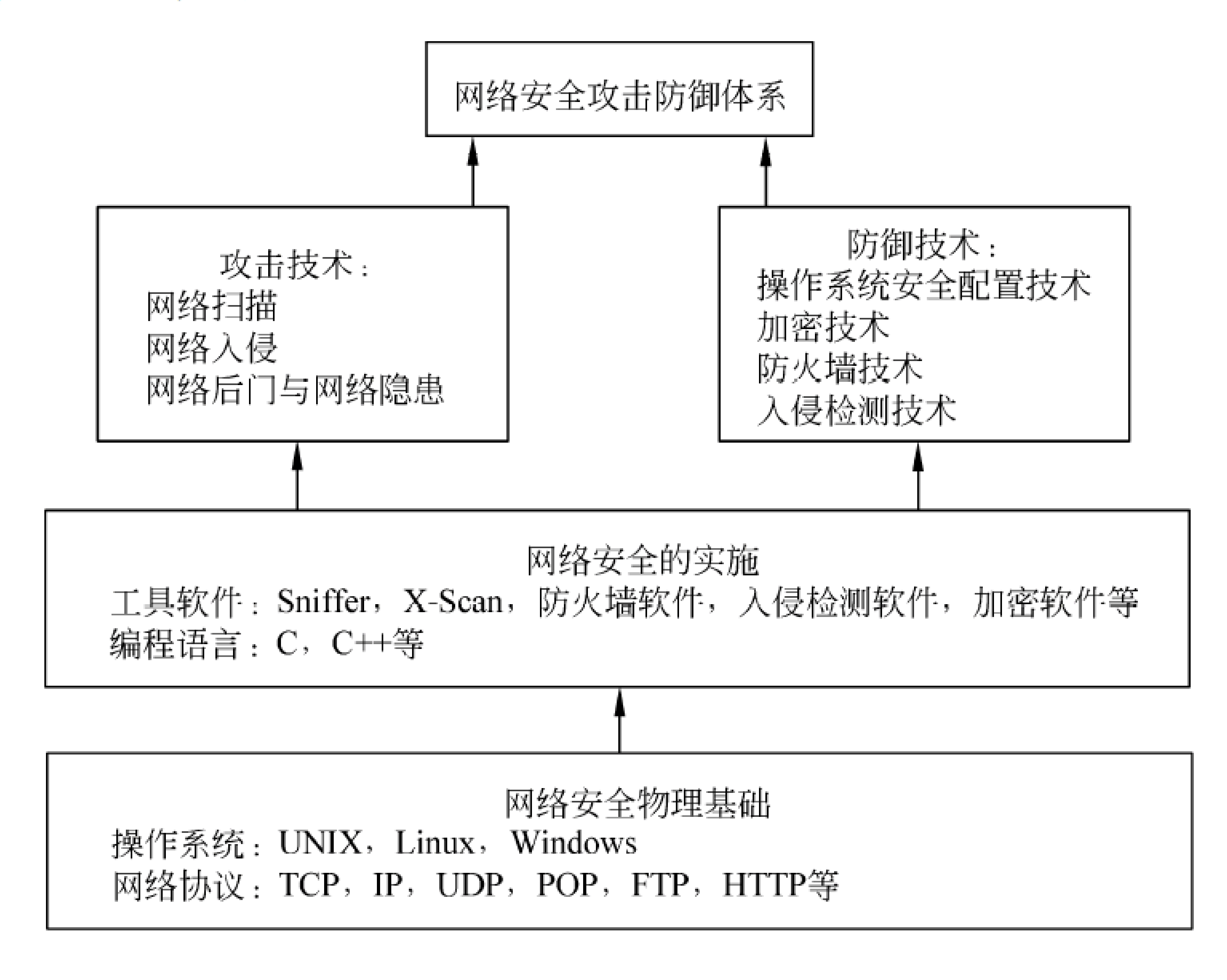


图 1-3　网络安全攻防体系结构

- **网络扫描**　利用程序去扫描目标计算机开放的端口等，目的是发现漏洞，为入侵该计算机作准备。
- **网络入侵**　当探测发现对方计算机存在漏洞以后，入侵到目标计算机以获取信息。
- **网络后门**　成功入侵目标计算机后，为了对“战利品”进行长期控制，在目标计算机中种植木马等。
- **网络隐身**　入侵完毕退出目标计算机后，将自己入侵该计算机的痕迹清除掉，从而防止被对方管理员发现。

对于防御技术通常包括以下 4 个方面。

- **操作系统的安全配置**　操作系统的安全是整个网络安全的关键。
- **加密技术**　为了防止被他人（非法分子）监听和盗取数据，通过加密技术将所有的数据进行加密。
- **防火墙技术**　利用防火墙，对传输的数据进行限制，从而防止系统被入侵或者是减小被入侵的成功率。
- **入侵检测**　如果网络防线最终被攻破了，需要及时发出被入侵的警报。

另外，为了保证网络的安全，用户在软件方面可以选择在技术上已经成熟的安全辅助工具，如抓数据包软件 Sniffer，网络扫描工具 X-Scan 等。另外，如果用户具有较高的编程能力，还可以选择自己编写程序。目前，有关网络安全编程常用的计算机语言有 C、C++或者 Perl 等。

1.1.4　层次体系结构

从层次体系结构上，通常将网络安全划分成物理安全、逻辑安全、操作系统安全和联网安全 4 个层次。

1. 物理安全

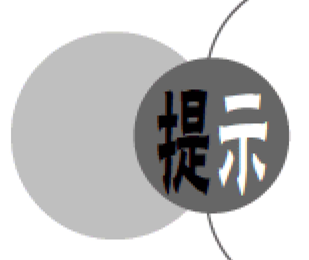
物理是指计算机硬件、网络硬件设备等。而物理安全是指整个计算机硬件、网络设备和传输介质等一些实物的安全。通常物理安全包括如下 5 个方面。

❑ **防盗**

与其他的物体一样，物理设备（如计算机）也是偷窃者的目标之一，如盗走硬盘、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施以确保计算机设备不会丢失。

❑ **防火**

计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。



人为事故是指由于操作人员不慎如吸烟、乱扔烟头等，使存在易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火蔓延到机房而引起火灾。

❑ **防静电**

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电放电火花，造成火灾。还可能使大规模集成电器损坏，这种损坏可能是不知不觉造成的。

❑ **防雷击**

利用传统的避雷针防雷，不但增加雷击概率，还会产生感应雷，而感应雷是电子信息设备被损坏的主要原因之一，也是易燃易爆品被引燃引爆的主要原因。

目前，对于雷击的主要防范措施是根据电气、微电子设备的不同功能及不同受保护程序和所属保护层来确定防护要点作分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应作多层保护。

❑ **防电磁泄露**

与其他电子设备一样，计算机在工作时也要产生电磁发射。电磁发射包括辐射发射和传导发射两种类型。而这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，从而会造成计算机中信息的泄露。

目前，屏蔽是防电磁泄露的有效措施，屏蔽方式主要包括电屏蔽、磁屏蔽和电磁屏蔽 3 种类型。

2. 逻辑安全

计算机的逻辑安全需要用口令、文件许可等方法来实现。例如，可以限制用户登录的次数或对试探操作加上时间限制；可以用软件来保护存储在计算机文件中的信息。

限制存取的另一种方式是通过硬件完成的，在接收到存取要求后，先询问并校核口令，然后访问位于目录中的授权用户标志号。

另外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如，多次登录或请

求别人的文件。

3. 操作系统安全

操作系统是计算机中最基本、最重要的软件。而且在同一台计算机中，可以安装几种不同的操作系统。例如，一台计算机中可以安装 Windows 7 和 Windows XP 两种系统，从而构成双系统。

如果计算机系统可提供给许多人使用，操作系统必须能区分用户，以避免用户间相互干扰。一些安全性较高、功能较强的操作系统（如 Windows Server 2008）可以为计算机的每一位用户分配账户。通常，一个用户一个账户。操作系统不允许一个用户修改由另一个账户创建的数据。

4. 联网安全

联网安全是指用户使用计算机与其他计算机通信的安全，通常由以下两个方面的安全服务来达到。

- **访问控制服务**　用来保护计算机和联网资源不被非授权使用。
- **通信安全服务**　用来认证数据机要性与完整性，以及各通信的可信赖性。

1.1.5　安全管理

随着网络技术的快速发展，与其相关的领域也发生了巨大变化，一方面，硬件平台、操作系统、应用软件变得越来越复杂和难以实行统一管理；另一方面，现代社会生活对网络的依赖程度逐渐加大。因此，如何合理地管理网络变得至关重要。

网络管理包括监督、组织和控制网络通信服务，及信息处理所必须的各种技术手段和措施。网络管理是为了确保计算机网络系统的正常运行，并在其出现故障时能及时响应和处理。

一般来讲，网络管理的功能包括配置管理、性能管理、安全管理和故障管理 4 个方面。由于网络安全对整个网络的性能及管理有着很大的影响，因此已经逐渐成为网络管理技术中的一个重要组成部分。

网络管理主要偏向于对网络设备的运行状况、网络拓扑、信元（Cell）等的管理，而网络安全管理则主要偏向于网络安全要素的管理。其中，网络安全管理主要包括安全配置、安全策略、安全事件和安全事故 4 个要素内容。

1. 安全配置

安全配置是指对网络系统各种安全设备、系统的各种安全规则、选项和策略的配置。它不仅包括防火墙系统、入侵检测系统、虚拟专用网（VPN）等安全设备方面的安全规则、选项和配置，而且也包括各种操作系统、数据库系统等系统配置的安全设置和优化措施。

安全配置能否很好地实现将直接关系到安全系统发挥作用的能力。若配置得好，就能够充分发挥安全系统和设备的安全作用，实现安全策略的具体要求；若配置得不好，不仅不能发挥安全系统和设备的安全作用，还可能起到副作用，如出现网络阻塞，网络运行速度下降等情况。

安全配置必须得到严格的管理和控制，不能被他人随意更改。同时，安全配置必须备案存档，必须做到定期更新和复查，以确保其能够反映安全策略的需要。

2. 安全策略

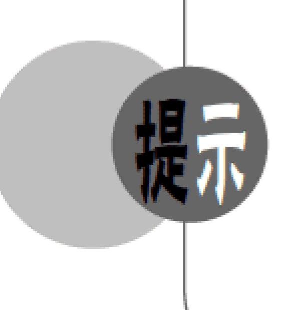
安全策略是由管理员制定的活动策略，基于代码所请求的权限为所有托管代码以编程方式生成授予的权限。对于要求的权限比策略允许的权限还要多的代码，将不允许其运行。前面提到的安全配置正是对安全策略的微观实现，合理的安全策略又能降低安全事件的出现概率。安全策略的设施包括如下 3 个原则。

- **最小特权原则** 它是指主体在执行操作时，将按照其所需权利的最小化原则分配权利的方法。
- **最小泄露原则** 它是指主体执行任务时，按照主体所需要知道的信息最小化的原则分配给主体权利。
- **多级安全策略** 它是指主体与客体之间的数据流向和权限控制按照安全级别绝密（TS）、秘密（S）、机密（C）、限制（RS）和无级别（U）这 5 个等级来划分。

3. 安全事件

事件是指那些影响计算机系统和网络安全的不正当行为。它包括在计算机和网络上发生的任何可以观察到的现象以及用户通过网络进入到另一个系统以获取文件、关闭系统等。恶意事件是指攻击者对网络系统的破坏，如在未经授权的情况下使用合法用户的账户登录系统或提高使用权限、恶意篡改文件内容、传播恶意代码、破坏他人数据等。

安全事件是指那些遵守安全策略要求的行为。它包括各种安全系统和设备的日志及事件、网络设备的日志和事件、操作系统的日志和事件、数据库系统的日志和事件、应用系统的日志和事件等方面内容。另外，它能够直接反应网络、操作系统、应用系统的安全现状和发展趋势，是对网络系统安全状况的直接体现。



计算机系统和网络的安全从小的方面说是计算机系统和网络上数据与信息的保密性，完整性以及信息、应用、服务和网络等资源的可用性；从大的方面来说，越来越多的安全事件随着网络的发展而出现，比如电子商务中抵赖、网络扫描、骚扰性行为、敲诈、传播色情内容，有组织的犯罪活动、欺诈、愚弄，所有不在预料之内的对系统和网络的使用和访问均有可能导致违反既定安全策略的安全事件。

由于安全事件数量多、分布不均及技术分析较复杂，导致其难以管理。在实际工作中，不同的系统又由不同的管理员进行管理。面对大量的日志和安全事件，系统管理员根本就没有时间和精力对其进行察看和分析，致使安全系统和设备的安装形同虚设，没有发挥其应有的作用。所以，安全事件是网络安全管理的重点和关键。

4. 安全事故

安全事故是指能够造成一定影响和损失的安全事件，它是真正的安全事件。一旦出现安

全事故，网络安全管理员就必须采取相应的处理措施和行动来阻止和减小事故所带来的影响和损失。

在出现安全事故时，管理员必须及时找出发生事故的源头、始作俑者及其动机并准确、迅速地对其进行处理。另外，必须要有信息资产库和强大的知识库来支持，以保证能够准确地了解事故现场系统或设备的状况和处理事故所需的技术、方法和手段。

1.1.6　安全目标

网络信息安全的目标是保护网络信息系统，使其减少危险、不受威胁、不出事故。从技术角度来说，主要表现在系统的可靠性、保密性、完整性、认证、可用性以及不可抵赖性等方面。

现在计算机网络安全的目标是：均衡考虑安全和通信方便性。显然，要求计算机系统越安全，则对通信的限制和使用的难度就越大。而现代信息技术的发展又使通信成为不可缺少的内容，它包括跨组织、跨学科、跨地区以及全球的通信。

一般来说，公司或其他经营单位的安全措施应包括如下 3 个主要目标。

- 对数据存取的控制。
- 保持系统及数据的完整性。
- 能够对系统进行恢复和对数据进行备份（在系统发生故障时）。

换句话说，一种安全的信息技术系统要对用户的访问权限予以限制，同时避免应用软件或数据的破坏，更重要的是当系统失灵时能够重新启动系统并保存重要数据的备份。

计算机安全的重要性是毫无疑问的。但是计算机的安全程度应与所涉及的信息的价值相适应。应当有一个从低、中到高级的多层次的安全系统，分别对不同重要性的信息资料给予不同级的保护。

1. 维护隐私

一个拥有存储个人和财务信息数据库的公司、医院和其他机构都需要维护隐私，这不仅是为了保护他们客户的利益，而且也是为了维护他们自己公司的利益和可信性。

要维护存储在一个单位或公司网络上信息的隐私，最重要和最有效的方法之一就是向普通员工讲授安全风险和策略。这种增强自我意识的教育并非他们考虑的一项事项，但它却是一项应当实现的重要任务。毕竟有个别员工很可能会进行检测，甚至由于他们自己粗心的行为而无意中造成安全隐患。他们还能够监控同事的活动，并且可能会了解到一些人在下班后复制文件、一些人在家里使用不安全的连接访问的网络，或者一些其他可疑的活动。

2. 保持数据的完整性

通常入侵者或破坏者会将虚假信息输入 Internet 或者在使用 TCP/IP 的网络上传输数据的数据包中。黑客能够使电子邮件看起来就像是来自正在接收它们的人，或者来自于一家受信任的公司。

当破坏性或伪造的数据包到达网络的外围时，防火墙、杀毒软件和入侵检测系统（IDS）都可以阻挡它们。但是，确保网络安全的一种更加有效的方法是在网络的关键位置就使网络

通信免受剽窃或伪造，从而保持通信的完整性。

利用在Internet上使用的多种加密方法中的任意一种，都可以保持数据的完整性。目前，最流行的方法之一是使用公钥加密技术，它使用一种称为密钥的长代码块加密通信。网络上的每个用户都可以获得一个或多个密钥，它们是由称为算法的复杂公式生成的。

3. 验证用户

21 世纪网络安全最基础和最重要的方面之一就是从防御网络（重点放在防御措施和限制访问的网络）转变到信任网络（允许那些身份通过可靠验证的信任用户访问的网络）。

为此，可以设置防火墙，这样就可以迫使用户在访问联网服务器时必须输入用户名和口令。通过匹配用户名和口令或者其他方法来确定授权用户身份的过程称为身份验证。有时可以对代理服务器（为用户提供 Web 浏览、电子邮件和其他服务的程序，以便对网络之外的用户隐藏他们的身份）进行设置，这样当用户利用 Web 上网冲浪或使用其他基于 Internet 的服务之前，代理服务器将要求进行身份验证。

4. 支持连接性

在Internet的早期，网络安全主要强调的是阻止黑客或其他未经授权用户访问公司的内部网络。然而，随着 Internet 用户的快速增长，通过 Internet 进行的业务量也越来越多，因此，这些企业（或其他消费用户）经常要进行的许多活动都可能会被黑客或罪犯分子利用，所以现在最需要的是与信任用户和网络的连接性。

黑客或其他犯罪分子通常会通过以下手段来进行非法活动。

- 直接访问对方企业的信息系统下订单，而不再通过电话或传真。
- 利用 Internet 电子银行转账的方式付款。
- 查找员工的记录。
- 为需要访问网络的职员创建口令。

为了保证这类业务的安全性，许多企业的传统做法就是建立租用线路。租用线路是由拥有连接线路的电信公司建立的点对点连接或其他连接。这种方式非常安全，因为它们直接将两个企业网络连接起来，其他公司或用户不能使用该电缆或连接。但是租用线路的价格非常昂贵。

为了削减成本，许多已经具有与 Internet 高速连接的企业建立了虚拟专用网络（VPN）。VPN 使用加密、身份验证和数据封装，数据封装是将数字信息的数据包装入另一个数据包从而保护前者的过程。这些 VPN 可以在使用 Internet 的计算机或者网络之间建立安全的连接。数据通过公众使用的同一个 Internet 从一个 VPN 参与者传输到另一个 VPN 参与者。不过，数据由各种安全措施进行安全保护。

- 在 VPN 连接的每一端都可以使用防火墙阻挡未授权的通信。
- AAA 服务器可以对通过 VPN 拨号进入受保护网络的用户进行身份验证。它们之所以被称为 AAA 服务器，是由于它们确定拨入的用户是谁（身份验证），确定允许用户在网络上进行什么活动（授权），并且记录用户在连接期间实际进行了什么活动（审计）。
- VPN 可以用多种数据加密方法。这些方法包括日益流行的 Internet 协议的安全(IPSec)，可以在计算机、路由器和防火墙之间加密数据，并且使用加密和身份验证使数据沿着

VPN 安全地传输。数据以传送模式或隧道模式沿着 VPN 发送，这两种模式都加密 TCP/IP（传输控制协议/Internet）数据包的数据有效负载。

数据受到高度保护的事实是建立了和虚拟“通道”一样安全的连接，如图 1-4 所示。

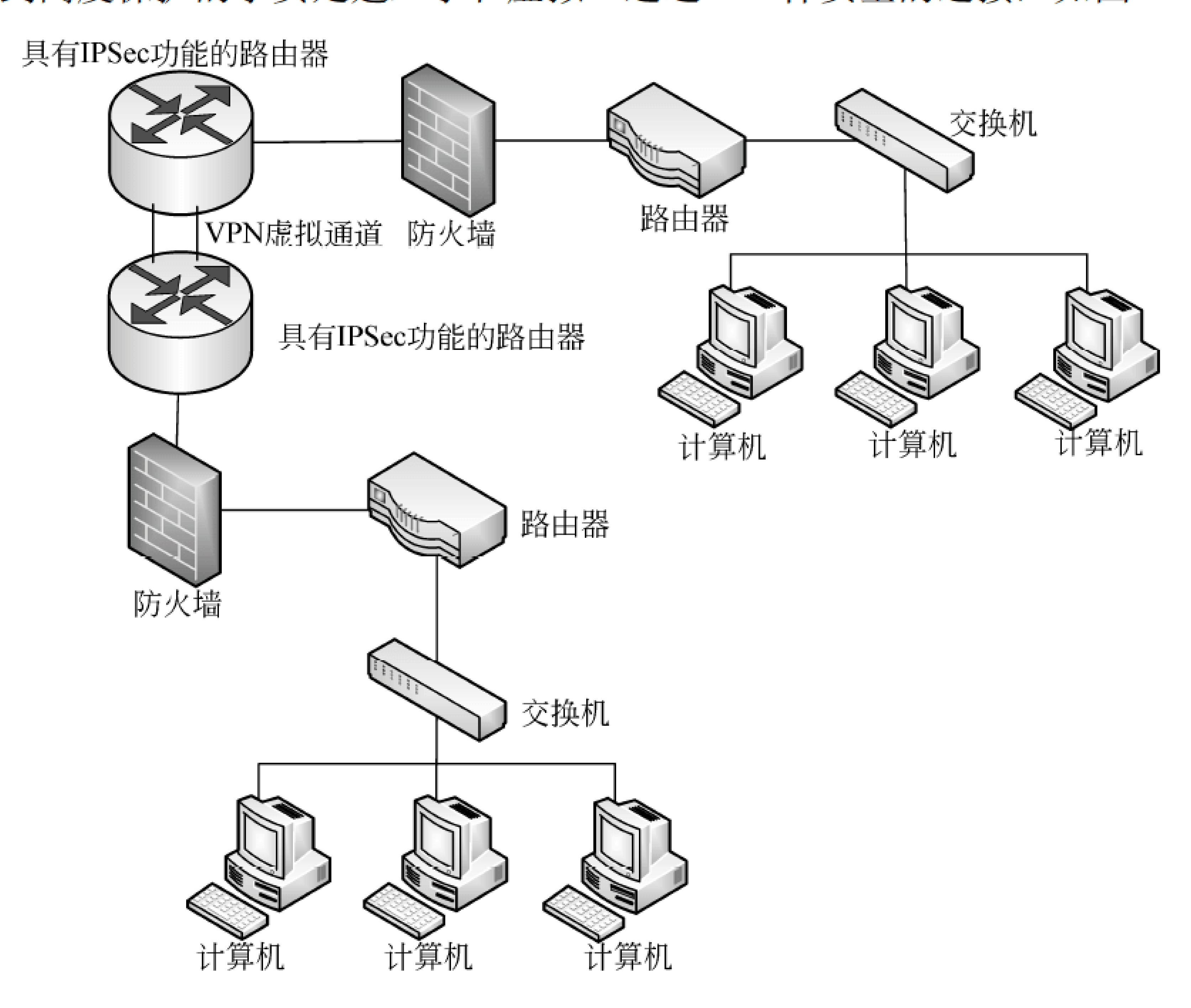


图 1-4　通过 VPN 提供安全连接

1.2　网络安全评价标准

评价标准中比较流行的是 1985 年由美国国防部制定的可信计算机系统评价准则（Trusted Computer Standards Evaluation Criteria，TCSEC），而其他国家也根据各自的国情制定相关的网络安全评价标准。

1.2.1　国内评价标准

在我国根据《计算机信息系统安全保护等级划分准则》，1999 年 10 月经过国家质量技术监督局批准发布的准则将计算机安全保护划分为以下 5 个级别。

❑ **第一级**

用户自主保护级，本级的计算机防护系统能够把用户和数据隔开，使用户具备自主的安全防护的能力。用户可以根据需要采用系统提供的访问控制措施来保护自己的数据，避免其他用户对数据的非法读写与破坏。

❑ **第二级**

系统审计保护级，与第一级（用户自主保护级）相比，本级的计算机防护系统访问控制

更加精细，使得允许或拒绝任何用户访问单个文件成为可能，它通过登录规则、审计安全性相关事件和隔离资源，使所有的用户对自己行为的合法性负责。

❑ 第三级

安全标记保护级，在该级别中，除继承前一个级别（系统审计保护级）的安全功能外，还提供有关安全策略模型、数据标记以及严格访问控制的非形式化描述。系统中的每个对象都有一个敏感性标签，而每个用户都有一个许可级别。许可级别定义了用户可处理的敏感性标签。系统中的每个文件都按内容分类并标有敏感性标签。任何对用户许可级别和成员分类的更改都受到严格控制。

❑ 第四级

结构化保护级，本级计算机防护系统建立在一个明确的形式化安全策略模型上，它要求第三级（安全标记保护级）系统中的自主和强制访问控制扩展到所有的主体（引起信息在客体上流动的人、进程或设备）和客体（信息的载体）。系统的设计和实现要经过彻底的测试和审查。系统应结构化为明确而独立的模块，实施最少特权原则。必须对所有目标和实体实施访问控制政策，要有专职人员负责实施。要进行隐蔽信道分析，系统必须维护一个保护域，保护系统的完整性，防止外部干扰。系统具有相当的抗渗透能力。

❑ 第五级

访问验证保护级，本级的计算机防护系统满足访问监控器的需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机防护系统在其构造时，排除那些对实施安全策略来说并非必要的部件，在设计和实现时，从系统工程角度将其复杂性降到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

我国是国际化标准组织（International Standardization Organization，ISO）的成员国，信息安全标准化工作在全国信息技术标准化技术委员会、信息安全技术委员会和社会各界的努力下正在积极开展。从 20 世纪 80 年代中期开始，我国就已经自主制定和采用了一批相应的信息安全标准。但是，标准的制定需要较为广泛的应用经验和较为深入的研究背景，相对于国际上其他发达国家信息技术安全评价标准来讲，我国在这方面的研究还存在差距，较为落后，仍需要进一步提高。

1.2.2 美国评价标准

美国计算机安全标准是由美国国防部开发的计算机安全标准——可信计算机系统评价准则，也称为网络安全橙皮书，主要通过一些计算机安全级别来评价一个计算机系统的安全性。

在该标准中定义的安全级别描述了计算机不同类型的物理安全、用户身份验证（Authentication）、操作系统软件的可信任度和用户应用程序。同时，也限制了什么类型的系统可以连接到用户的系统。

另外，该准则自 1985 年问世以来，一直就没有改变过，多年来一直是评估多用户主机和小型操作系统的主要标准。其他方面，如数据安全、网络安全也一直是通过该准则来评估的。如可信任网络解释（Trusted Network Interpretation）、可信任数据库解释（Trusted Database Interpretation）。TCSEC 将安全级别从低到高依次划分为 D 类、C 类、B 类和 A 类 4 个安全级别，每类又包括几个级别，如表 1-1 所示。

表 1-1　安全级别

类别	级别	名称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储介质	单独的可查性，安全标识
B	B1	标识的安全防护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控，高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

1. D 级

D 级是该标准中最低的安全级别，该级说明整个系统是不可信的。换句话说，拥有这个级别的操作系统就像一个门户大开的房子，任何人都可以自由进出，是完全不可信任的。

对于硬件来说，没有任何保护作用；对于操作系统来说较容易受到损害；对于用户和他们存储在计算机上的信息来讲，没有系统访问限制和数据访问限制，任何人不需要账户都可以进入系统，不受限制就可以访问他人的数据文件。

属于该安全级别的操作系统都是早期的操作系统，如 MS-DOS、Windows 98 和 Apple 的 Macintosh System 7.X 等。这些操作系统不区分用户，并且没有定义一种方法来决定谁来操作，这些操作系统对计算机硬盘上的信息都可以访问，而没有控制。

2. C 级

C 级安全级别能够提供审慎的保护功能，并具有对用户的行为和责任进行审计的能力。该安全级别又由 C1 和 C2 两个子安全级别共同组成。

- **C1**

C1 安全级别又称为选择性安全保护（Discretionary Security Protection）系统，描述了一个典型的用在 UNIX 系统上安全级别。

该级别对于硬件来说存在某种程度上的保护，因此不那么容易受到损害。如用户拥有注册账号和口令，系统则通过该账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权，但硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件和目标的访问权。文件的拥有者和超级用户可以改变文件的访问属性，从而对不同的用户授予不同的访问权限。

- **C2**

C2 级除 C1 级包含的特性外，还具有访问控制环境（Controlled Access Environment）的安全特征。访问控制环境具有进一步限制用户执行某些命令或访问某些文件的能力，这不仅仅是基于许可权限，而且还基于身份验证级别。这种级别要求对系统加以审核，并写入日志中，例如，用户何时开机、哪个用户在何时何地登录系统等。通过查看日志信息，就可以发现入侵的痕迹，如发现多次登录失败的日志信息，那么可大致得出有人想入侵系统。

另外，审核用来跟踪记录所有与安全有关的事件，比如系统管理员所执行的操作活动，审核对身份的验证。审核的缺点就是需要额外的处理器和磁盘空间。

使用附加身份验证就可以让一个 C2 级系统用户在不是超级用户的情况下有权执行系统

管理任务。授权分级使系统管理员能够给用户分组，授予他们访问某些程序的权限或访问特定的目录。能够达到 C2 级别的常见操作系统有如下几种类别。

- UNIX 系统。
- Novell 3.X 或者更高版本。
- Windows NT、Windows 2000 和 Windows Server 2003。

3. B 级

B 类安全等级可分为 B1、B2 和 B3 3 个子安全级别。B 类系统具有强制性保护功能，强制性保护意味着如果用户没有与安全等级相连，系统就不会允许用户存取对象。

- **B1**

B1 级也称为标志安全保护（Labeled Security Protection），是支持多级安全（如秘密和绝密）的第一个级别。这一级说明一个处于强制性访问控制之下的对象，不允许文件的拥有者改变其许可权限。



安全级别存在保密、绝密级别，这种安全级别的计算机系统一般用于政府机构中，比如国防部和国家安全局的计算机系统。

- **B2**

B2 级又称为结构保护（Structures Protection）级别，要求计算机系统中所有对象都要加注标签，而且还要给设备（如磁盘、磁带等）分配单个或多个安全级别。这样构成了一个由较高安全级别的对象与另一个较低安全级别的对象通信的级别。

- **B3**

B3 级又称为安全域（Security Domain）级别，使用安装硬件的方式来加强域的安全。例如，安装内存管理硬件用于保护安全域免遭无授权访问或更改其他安全域的对象。这种级别也要求用户的终端通过一条可信任的途径连接到系统上（如防火墙技术）。

4. A 级

A 级又称为验证设计（Verified Design）级别，是当前橙皮书的最高级别，包含一个严格的设计、控制和验证过程。该级别包含了较低级别的所有的安全特性。

安全级别设计必须从数学角度上进行验证，而且必须进行秘密通道和可信任分布分析。可信任分布（Trusted Distribution）的含义是：硬件和软件在物理传输过程中受到保护以防止破坏安全系统。

另外，橙皮书也存在不足。橙皮书是针对孤立计算机系统，特别是小型机和主机系统。假设有一定的物理保障，该标准适合政府和军队，不适合企业，这个模型是静态的。

1.2.3 加拿大评价标准

在欧洲研究和发展计算机安全评估标准的同时，加拿大也开始了这方面的研究，1988 年 8 月，加拿大系统安全中心（Canadian System Security Center，CSSC）成立，主要任务是开放能满足加拿大政府的独特要求的标准和提高加拿大的评估计算机系统安全的能力。

最早的加拿大标准“加拿大可信任计算机产品评估标准（Canadian Trusted Computer Product Evaluation Criteria，CTCPEC）”于 1989 年 5 月公布，1990 年 12 月推出了 2.0 版本，1991 年 7 月推出了 2.1 版本，并于 1993 年推出了 3.0 版本。CTCPEC 3.0 版本综合了欧洲 ITSEC 和美国 TCSEC 的优点。

提示

在美国发表 TCSEC 之后，欧洲各国就开始对信息技术的安全问题进行研究，并且发表了自己的信息技术安全评价标准。1991 年，由德国、法国、荷兰和英国共同合作并发表了“信息技术安全评价标准（Information Technology Security Evaluation Criteria，ITSEC）”的共同标准。

美国的 TCSEC 主要针对的是多用户大型机和小的操作系统。而对于数据库、网络和子系统等都只是进行解释说明，例如，可信数据库解释、可信网络解释。为了避免使用解释条款，加拿大标准针对的目标更加广泛，包括大型机、多处理系统、数据库、嵌入式系统、分布式系统、网络系统和面向对象系统等。

加拿大的安全标准对开发的产品或评估过程强调功能和保证两个部分。

❑ 功能（**Functionality**）

功能包括保密性、完整性、可用性和审核 4 个方面的标准。这 4 个标准之间可能存在一些相互依赖关系，如果这些标准在不同服务之间存在相互依赖关系，这种关系称为约束。

❑ 保证（**Assurance**）

保证包含保证标准，是指产品用以实现组织的安全策略的可信度。保证标准评估是对整个产品进行的。如一个被评为 T-4 保证级别的标准，那么它所提供的每个服务都能达到该标准要求。

CTCPEC 标准制定的较为细致，它的功能标准中的每个服务都具有不同的级别，表 1-2 列出了它的不同标准中服务的级别。

表 1-2　加拿大 CTCPEC 中的标识和级别

标准	字母符号	全称	范围
保密性（Confidentiality）	CC	转换通道（Convert Channels）	CC0～CC3
	CD	任意保密性（Discretionary Confidentiality）	CD0～CD4
	CM	强制保密性（Mandatory Confidentiality）	CM0～CM4
	CR	对象重用（Object Reuse）	CR0～CR1
完整性（Integrity）	IB	域完整性（Domain Integrity）	IB0～IB2
	ID	任意完整性（Discretionary Integrity）	ID0～ID4
	IM	强制完整性（Mandatory Integrity）	IM0～IM4
	IP	物理完整性（Physical Integrity）	IP0～IP4
	IR	回滚（Rollback）	IR0～IR2
	IS	责任分离（Separate Of Duties）	IS0～IS3
	IT	自我检测（Self Testing）	IT0～IT3
可用性（Availability）	AC	封装（Containment）	AC0～AC3
	AF	容错性（Fault Tolerance）	AF0～AF3
	AR	健壮度（Robustness）	AR0～AR2
	AY	恢复（Recovery）	AY0～AY3

续表

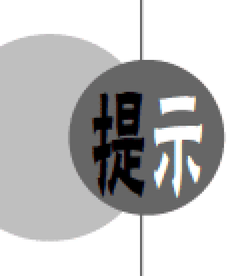
标准	字母符号	全称	范围
可审核度（Accountability）	WA	审计（Audit）	WA0～WA5
	WI	身份认证（Identification and Authentication）	WI0～WI3
	WT	信任通道（Trusted Path）	WT0～WT3
保证度	T	保证度（Assurance）	T0～T7

1.2.4 美国联邦标准

1993 年，美国国家标准和技术研究所（National Institute of Standard and Technology，NIST）和国家安全局（National Security Agency，NSA）联邦标准（Federal Criteria，FC）项目组联合发布了信息技术安全联邦标准（Federal Criteria for Information Technology Security）。

美国联邦标准综合了欧洲的 ITSEC 和加拿大的 CPCETC 的优点，用来代替原来的橙皮书 TCSEC，成为新的联邦信息处理标准（Federal Information Processing Standard，FIPS）。

这个标准引入了保护轮廓（Protection Profiles）的概念。保护轮廓是以通用要求为基础创建的一套独特的 IT 产品安全标准。它是关于 IT 产品安全方面的抽象描述，但却独立于产品，描述了符合这个安全需求的某一类产品。另外，保护轮廓需要对设计、实现和使用 IP 产品的要求进行详细说明。通常，保护轮廓由如下 5 个方面构成。



IT 英文全称为“Information Technology，信息技术”，包括硬件、软件和应用 3 个层次。其中，硬件主要是指数据存储、处理和传输的主机和网络通信设备；软件包括可用来搜集、存储、检索、分析、应用、评估信息的各种软件，既包括企业资源计划（ERP）、CRM 客户关系管理（CRM）等商用管理软件，也包括用来加强流程管理的工作流（WF）管理软件、辅助分析的数据仓库和数据挖掘（DW/DM）软件等；应用是指搜集、存储、检索、分析、应用、评估使用的各种信息，

1. 描述元素

描述元素提供明确、分类、记录和交叉引用等描述性信息。描述性的说明要阐述轮廓的特性，以及要解决的问题。

2. 基本原理

基本原理部分提供保护轮廓的基本定位，包括威胁、环境和使用假设。另外，基本原理还进一步说明符合这个要求的一个 IT 产品要解决的安全问题的详细特征。

3. 功能要求

功能要求部分用来建立 IT 产品要提供的信息保护范围。在这个范围之内对信息的威胁必须和这个范围之内的保护功能相对应。从理论上讲，威胁越大，保护功能越强。

4．开发保证要求

开发保证要求部分包含 IT 产品的所有开发阶段，从初始的产品设计到实现。特别是开发保证要求包含开发过程、开发环境和操作支持环境。

另外，由于多数的开发保证要求是随时可以测试的，因此必须检查产品开发的证据或者是文档，以表明保证要求已经达到，且这些证据或文档需要保留，供以后评估使用。

5．评估保证部分

评估保证部分要求详细说明对某一产品要进行怎样的评估，包括评估的类型和强度，通常评估的类型和强度会随着基本原理所描述的预期威胁、预期使用方法和假象环境的不同而不同。

1.2.5　共同标准

由于较多的安全标准都没有得到广泛的承认，国家标准化组织于 1990 年开始着力于研究一个共同标准。直到 1993 年，德国、法国、荷兰、英国、加拿大和美国这 6 个国家的 7 个部门联合在一起，才将他们的标准组合成一个单一的全球标准，即信息技术安全评估共同标准（Common Criteria for Information Technology Security Evaluation，CCITSE），通常称为共同标准（Common Criteria，CC）。

1．绪论和总体模型

绪论和总体模型为 CC 的第一部分，该部分是对 CC 的介绍。它定义了安全评估的总体概念和原则并给出了一个总体的评估模型。

另外，第一部分给出描述 IT 安全目标、选择和定义 IT 安全要求、给产品和系统书写高级规范的结构。还说明 CC 的每个部分对哪些人有哪些作用。

2．安全功能要求

安全功能要求为 CC 的第二部分，建立了一套功能要求组件，作为表达评估对象功能要求的标准方法。

3．安全保证要求

安全保证要求为 CC 的第三部分，建立了一套保证组件，作为表达评估对象保证要求的标准方法。其中，也给出了已经定义好的 CC 评估保证级别（Evaluation Assurance Level，EAL）。

CC 评估保证级别通常有 7 个保证级，称为 EAL 1～EAL 7。

❑ **EAL 1 保证级**

EAL 1 保证级为最低的保证级别，它对开发人员和用户来说是有意义的。它定义了最小程度的保证，以产品安全性能分析为基础，并以使用功能和接口设计来理解安全行为。

❑ **EAL 2 保证级**

EAL 2 保证级是在不需要强加给产品开发人员除 EAL 1 要求的任务之外的附加任务的情况下，可授予的最高的保证级别。它执行对功能和接口规范的分析以及对产品子系统的高级

设计检查。

❑ **EAL 3 保证级**

EAL 3 保证级是一种中间的独立确定的安全级别，就是说安全要由外部源来证实。该级别允许设计阶段给予最大的保证，而测试过程中几乎不加修改。最大的保证是指在设计时已经考虑到了安全问题，而不是设计完之后再实现安全性，开发人员必须提供测试数据，包括易受攻击的分析，并有选择地加以验证。

❑ **EAL 4 保证级**

EAL 4 保证级是改进已有生产线可行的最高保证级别。它向用户提供了最高的安全级别，也是以良好的商业软件开发经验为基础的。除了具有 EAL 3 级的内容外，EAL 4 还包含对产品的易受攻击性进行独立的搜索。

❑ **EAL 5 保证级**

EAL 5 保证级对现有的产品来说是不易达到的，该级别使用于那些在严格的开发方法中要求较高保证级别的开发人员和用户。在这一级别上开发人员也必须提出设计规范和如何从功能上实现这些规范。

❑ **EAL 6 保证级**

EAL 6 保证级包含一个半正式的验证设计和测试主件，并包含 EAL 5 级的所有内容，除此之外还应提出实现的结构化表示。同时，产品要经受高级的设计检查，而且必须保证具有高度的抗攻击性能。

❑ **EAL 7 保证级**

EAL 7 保证级用于最高级别的安全应用程序。EAL 7 包含完整的、独立的和正式的设计、测试和验证。

1.2.6　网管心得——网络安全防范建议

网络安全是一个相对的而非绝对的概念，所以用户必须居安思危，时时作好防范准备。网络安全也是一个动态更新的过程，其对安全的威胁因素是不可能根除的，所以不能存在侥幸心理，应时刻保持警惕。为此，用户在使用计算机或网络时应具备一些安全防范意识。

1. 使用防火墙

防火墙（Firewall）是指隔离在信任网络（本地网络）与不可信任网络（外部网络）之间的一道防御系统。它是一种非常有效的网络安全系统，通过它可以隔离风险区域（Internet 或其他存在风险的网络）与安全区域（本地网络）的连接，而不会妨碍安全区域对风险区域的访问。

但是，在单位或公司的网络中，即使配置了防火墙，也不能保证该网络就是 100%安全的，因此不能而掉以轻心。

2. 主动防御

由于现在的防病毒软件、防火墙等防御措施都是被动的，它们都是在危险发生时才能发

挥其应有的作用，这对于系统来说是很不安全的。主动防御是指在明确病毒或其他危险活动所产生行为的基础上，对网络中数据行为进行分析，查找并终止类似病毒或其他危险活动行为的产生。

3．安装系统补丁

目前，黑客、病毒、木马等大部分危险因素都是利用系统漏洞，编写相应程序来实现入侵的。因此，及时安装系统补丁封堵系统漏洞也是保护网络安全的有效方法。

4．提高用户的安全意识

用户的安全意识在一定程度上对网络安全起着决定性的作用，因为大部分黑客对网络进行的攻击都是从用户作为首要目标。用户应该注意以下几个方面。

- 在发送信息时，应该确定接收方的真实身份。
- 使用强密码，不要使用简单的、确实存在的单词或个人生日等信息作为密码，因为攻击者通过口令探测工具很容易将其猜出。
- 不要将密码随意放在易被发现的位置。
- 养成定时更换密码的习惯。
- 不同操作系统或不同用户要使用完全不相同的密码。不能出现诸如 admin1、admin2 等这样只更改部分字符的密码。
- 对于使用过的文件应该使用文件粉碎机将其彻底粉碎，不能将文件随意丢弃。
- 适时对磁盘进行清理，以防留下曾经删除和改正等使用痕迹。

网络安全是一项艰巨的动态工程。它的安全程度会随着时间的推移而发生变化。在信息技术日新月异的今天，网络安全的实现要随着时间和网络环境的变化或技术的发展而不断调整自身的安全防范策略。

1.3　常见的安全威胁与攻击

计算机网络安全受到的威胁不仅包括“黑客”的攻击、计算机病毒和拒绝服务攻击（Denial of Service Attack），还包括常见的非授权访问、假冒合法用户、数据完整性受破坏和通信线路被窃听。

1.3.1　网络系统自身的脆弱性

网络系统自身由于系统主体和客体的原因可能存在不同程度的脆弱性，因此为各种动机的攻击提供了入侵、骚扰或破坏网络系统的途径和方法。网络系统自身的脆弱性是指网络系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因而可能导致系统受到破坏、更改、泄露和功能失效，从而使系统处于异常状态，甚至崩溃瘫痪等。

1. 硬件资源脆弱性

网络系统硬件资源的安全隐患来源于设计，主要表现为物理安全方面的问题。例如，各种计算机或网络设备（如主机、电缆、交换机、路由器等），除难以抗拒的自然灾害外，温度、湿度、尘埃、静电、电磁场等也可以造成信息的泄露或失效。

另外，网络系统在工作时，会向外辐射电磁波，易造成敏感信息的泄露。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在设计硬件或选购硬件时，应尽可能减少或消除这类安全隐患。

2. 软件资源脆弱性

软件资源的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余及软件过长、过大，不可避免地存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别；软件工程实现中造成的软件系统内部逻辑混乱，导致垃圾软件，从安全角度考虑这种软件是绝对不能用的。

3. 网络和通信协议脆弱性

当前计算机网络系统使用的 TCP/IP 协议以及 FTP、E-mail、NFS 中都包含着许多影响网络安全的因素，存在许多安全漏洞，主要有如下几方面的原因。

❑ **缺乏对通信双方真实身份的鉴别机制**

由于 TCP/IP 协议使用 IP 地址作为网络节点的唯一标识，而 IP 地址的使用和管理又存在很多问题，因而导致安全问题。

❑ **缺乏对路由协议的鉴别认证**

TCP/IP 在 IP 层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别与保护。因此，可以通过 Internet 利用路由信息修改网络传输路径，误导数据的传输。

❑ **TCP/UDP 协议的缺陷**

TCP/UDP 是基于 IP 协议上的传输协议，TCP 分段和 UDP 数据包是封装在 IP 包中在网络中传输的，因此可能面临 IP 层所遇到的安全威胁。

另外，建立一个完整的 TCP 连接，需要经历“三次握手”过程。在客户/服务器模式的“三次握手”过程中，假如客户机的 IP 地址是假的，是不可达的，那么 TCP 不能完成该次连接所需的“三次握手”，使 TCP 连接处于“半开”状态。因此，也会带来安全隐患。

4. 数据库管理系统安全的脆弱性

数据管理系统（DBMS）对数据库的管理是建立在分级管理的概念上的。因此，DBMS 的安全也是可想而知。另外，DBMS 的安全必须与操作系统的安全相配套，这是一个不足之处。

1.3.2 网络面临的安全威胁

网络威胁是对网络安全缺陷的潜在利用，这些缺陷可能导致非授权访问、信息泄露、资

源耗尽、资源被盗或者被破坏等。

由于网络需要与外界联系，因此也就受到许多方面的威胁，而且这些威胁随着时间的变化而变化。这些威胁包括物理威胁、系统存在安全漏洞所造成的威胁、身份鉴别威胁、线缆连接威胁及有害程序的威胁等，图 1-5 为它们相互关系示意图。

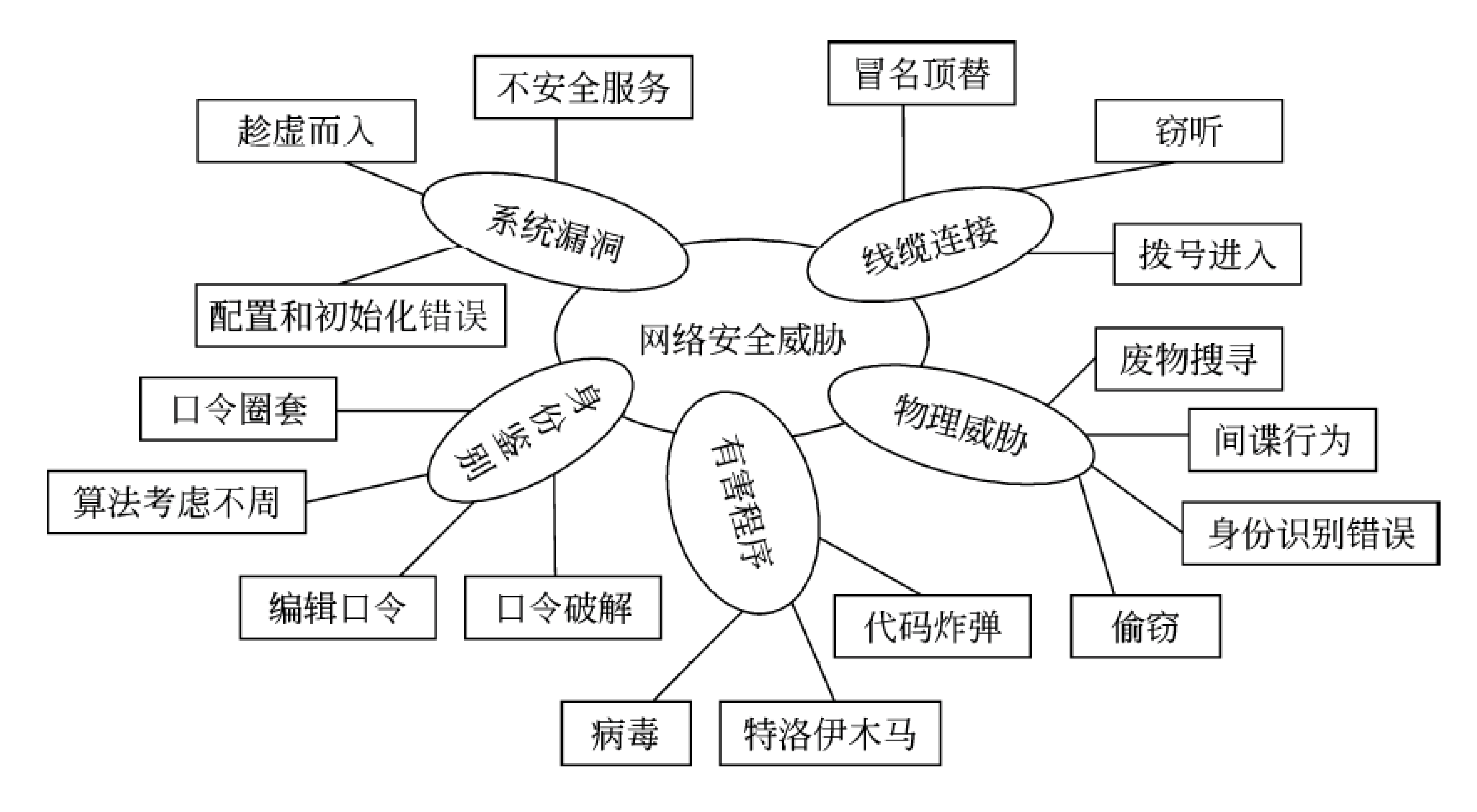


图 1-5　网络安全威胁类型

1. 物理威胁

物理安全是指用来保护计算机硬件和存储介质的装置和工作程序。有关物理威胁通常包括以下 4 个方面内容。

❑ 偷窃

网络安全中的偷窃包括偷窃物理设备、偷窃信息和偷窃服务等内容。例如，某人想要偷窃的信息存放在计算机中，一方面可以将整台计算机偷走，另一方面也可以通过监视器读取计算机中的信息。

❑ 废物搜寻

废物搜寻是指在人们遗弃不用的废物（如一些由打印机打印而不用的材料或废弃的磁盘等）中搜寻所需要的重要信息。在计算机上，废物搜寻可能包括从未格式化的软盘或硬盘中获取有用资料。

❑ 间谍行为

间谍行为是一种为了省钱或获取有价值的信息，而采用不道德的手段获取信息的方式。

❑ 身份识别错误

身份识别错误是指用户通过非法手段建立文件或记录，并企图将它们作为有效的、正式的文件或记录，从而对网络数据构成巨大威胁。例如，对那些具有身份鉴别特征的物品（如护照、执照、出生证明或加密的安全卡）进行伪装，属于身份识别错误的范畴。

2. 系统漏洞威胁

系统漏洞是指应用软件或操作系统软件在逻辑设计上存在的缺陷或在编写时产生的错误，这个缺陷或错误可以被不法者或者黑客利用，通过植入木马、病毒等方式来攻击或控制

整台计算机，从而达到窃取用户计算机中重要资料和信息，甚至破坏系统的目的。

具体来讲，系统漏洞可以造成如下 3 种威胁。

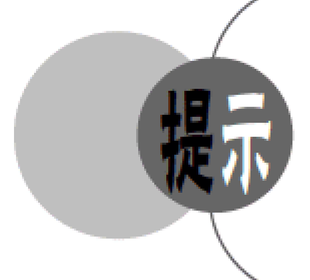
❑ **趁虚而入**

例如，某用户（A）停止了与某个系统的通信，但由于某种原因仍使该系统上的一个端口处于激活状态（未关闭），此时用户（B）通过这个端口进入该系统并与之通信，而不必通过申请使用端口的安全检查。从而带来安全隐患。

❑ **不安全服务**

在某些情况下，操作系统中存在不安全的服务，可以绕过计算机的安全检查机制，入侵者就可以利用这些不安全服务入侵系统，从而发生安全威胁。例如，互联网蠕虫就是利用 Berkeley Internet Name Domain（BIND）程序中存在的这种问题而直接得到管理员（root）权限。

另外，还有一类不安全网络服务是那些需要用户名和口令来验证的服务，如 Telnet 和 FTP 服务。如果有人使用嗅探软件监视远程用户和这类服务器间的连接，那么，用户的口令就能够被轻而易举地窃取。



在 UNIX 系统中，BIND 软件包是域名服务（DNS）中的一个应用最广泛的实现软件。如通过它，用户只需要知道某个网站的域名（如 www.baidu.com）而不必知道其 IP 地址就可以访问该网站。

❑ **配置和初始化错误**

在网络中，为了维护服务器或服务器中的某个部分，而关闭该服务器，但当几天后重新启动该服务器时，可能会发生用户文件丢失或被篡改的情况。这很可能就是系统在重新初始化时，安全系统没有正确初始化，从而留下了安全漏洞让人利用。另外，当木马程序修改系统的安全配置文件时也会发生这样的情况。

3. 身份鉴别威胁

身份鉴别一般是指计算机决定用户是否有权在服务器上进行操作（如复制、修改文件或文件夹等）或提供一些服务的过程。如果没有身份鉴别，网络就不会有安全。通常身份鉴别威胁包括如下 4 个方面。

❑ **口令圈套**

口令圈套是网络安全的一种诡计，与冒名顶替有关。常用的口令圈套通过一个编译代码模块来实现，运行起来和登录屏幕一模一样，被插入到正常登录过程之前，最终用户看到的只是先后两个登录屏幕，第一次登录失败了，所以用户被要求再次输入用户名和口令。实际上，第一次登录并没有失败，它将登录数据，如用户名和口令写入这个数据文件中，留待使用。

❑ **口令破解**

破解口令就好像人们猜测自行车或其他物品密码锁的数字组合一样，在该领域中已形成许多能提高成功率的技巧。

❑ **算法考虑不周**

口令输入过程必须在满足一定条件下才能正常地工作，这个过程通过某些算法实现。在

一些攻击入侵案例中，入侵者采用超长的字符串破坏口令算法，成功地进入计算机系统。

❑ **编辑口令**

编辑口令需要依靠操作系统漏洞，如某部门内部的人员建立一个虚设的账户或修改一个隐含账户的口令，这样知道该账户名称和口令的人员便可以访问该计算机了。

4．线缆连接威胁

随着网络技术的发展，网络线缆的连接对计算机数据造成了新的安全威胁，通常包括以下 3 个方面。

❑ **窃听**

窃听是指对通信过程进行窃听以达到收集信息的目的，这种电子窃听不需要窃听设备一定安装在线缆上，通过检测从连线上发射出来的电磁辐射就能获取所要的信号，为了使单位或公司内部的通信有一定的保密性，可以通过加密手段来防止信息被解密。

❑ **拨号进入**

拥有一个调制解调器（Modem）和一个电话号码，每个人都可以试图通过远程拨号访问网络，尤其是拥有所要攻击的网络的用户账户时，会对网络造成很大的威胁。

❑ **冒名顶替**

冒名顶替是指通过使用别人的密码和账号，来获得对网络及其数据、程序的使用能力。这种办法实现起来并不容易，而且一般需要有机构内部的、了解网络和操作过程的相关人员参与。

5．有害程序威胁

有害程序是一种能够危害计算机系统和网络安全的程序，通常这些有害程序都是由编程技术高超的用户编写，用以进行破坏操作及谋求个人利益。通常包括如下 3 个方面的威胁。

❑ **病毒**

病毒是一种把自己的备份附着于计算机中另一程序上的一段代码。通过这种方式病毒可以进行自我复制，并随着所附着的程序在计算机之间传播。

❑ **代码炸弹**

代码炸弹是一种具有杀伤力的代码，其运行原理是一旦达到了制作者所设定的日期或钟点，或用户在计算机中进行了某种操作，代码炸弹就会被触发并开始产生破坏性操作。代码炸弹不必像病毒那样四处传播。例如，程序员将代码炸弹写入软件中，使其产生了一个不能轻易被使用者找到的安全漏洞，一旦该代码炸弹被触发后，该程序员便会被请来修正这个错误，并赚到一笔钱，这种高技术的敲诈使受害者不知道被敲诈了，即便有疑心也无法证实自己的猜测。

❑ **特洛伊木马**

特洛伊木马程序一旦被安装到计算机中，便可按照编制者的意图运行。特洛伊木马能够摧毁数据，有时伪装成系统上已有的程序，有时创建新的用户名和口令。

1.3.3　网络安全面临威胁的原因

目前，无论是中小型企业还是大型企业，都开始广泛地利用信息化手段来提升自身的竞

争力。信息化网络可以有效提高中小企业的运营效率，使中小企业可以更快速地发展壮大。然而在获得这些利益的同时，网络信息的安全问题也给许多大型企业造成重大的损失，这同样也在困扰着中小型企业群体。虽然中小型企业的信息化设施规模相对较小，但是其面临的安全威胁却并不比大型企业少。前面已经讲过网络所面临的威胁，下面就来讲解网络安全面临威胁的原因。

1. 认证环节简单

计算机网络中采用的认证方式通常是采用口令来实现的。但口令比较薄弱，有多种方法可以破译，其中最常见的两种方法就是把加密的口令破解和通过信道窃取口令。例如，在 UNIX 操作系统中，通常是把加密的口令保存在某一个文件中，而该文件对于普通用户也是可以读取的。所以一旦该口令文件被入侵者通过简单复制的方式得到，他们就可以对口令进行解密，然后用它来取得对系统的访问权。

2. 通信易被监视

用户使用 Telnet 或 FTP 方式登录远程计算机时，需要输入用户名及密码，而在网络中传输的口令是未被加密的。因此，入侵者就可以通过监视携带用户名和密码的 IP 数据包从而获取它们，并使用这些用户名和密码登录系统。假如被截获的是管理员的用户名和密码，那么，获取该系统的超级用户访问就轻而易举了。

3. TCP/IP 协议未考虑安全因素

如果攻击者使用 IP Source Routing 命令，就可以冒充成为一个被信任的主机或者客户，从而危害网络。其实现过程有以下几个步骤。

- 使用被信任用户 IP 的地址取代自己的 IP 地址。
- 构造一条要攻击的服务器和其主机间的直接路径，把被信任用户作为通向服务器路径的最后节点。
- 利用此路径向服务器发送用户申请。
- 服务器接受用户申请，就好像是从可信任用户直接发出的一样，然后对可信任用户返回响应。
- 可信任用户使用这条路径将数据包向前传送给攻击者的主机。

4. 存在缺陷的局域网服务和相互信任的主机

计算机的安全管理不仅困难且费时。为了降低管理要求并增强局域网性能，一些站点使用了诸如网络信息服务（Network Information Services）和网络文件系统（Network Files System）之类的服务。这些服务通过允许一些数据库（如口令文件）以分布式方式管理，以及允许系统共享文件和数据，在很大程度上减轻了管理者的工作量。但这些服务也带来不安全因素，可以被有经验的闯入者利用以获得访问权。

另外，一些系统出于方便用户及加强系统和设备共享的目的，允许主机之间相互“信任”。这样，如果一个系统被入侵或欺骗，那么对于入侵者来说，获取信任该系统的其他系统的访问权就很简单。

5. 复杂的设置和控制

主机系统的访问控制配置复杂且难于验证。因此偶然的配置错误会使闯入者获取访问权。一些主要的 UNIX 经销商仍然把 UNIX 配置成具有最大访问权限的系统，这将导致未经许可的访问。许多网上的安全事故正是由于入侵者发现了其设置中的弱点而造成。

6. 无法估测主机的安全性

主机系统的安全性无法很好地估计。随着一个站点的主机数量增加，每台主机的安全性都处在高水平的能力却在下降。只用管理一台系统的能力来管理如此多的系统就容易犯错误。另一个因素是某些系统管理的作用经常变换并行动迟缓。这导致这些系统的安全性比另一些要低，使其成为网络中的薄弱环节，最终破坏了安全链。

1.3.4 网管心得——网络安全策略

网络安全涉及的问题非常多，如防病毒、防入侵破坏、防信息盗窃、用户身份验证等，这些都不是也不可能由单一产品来完成，它需要制定一个整体策略来解决，即网络安全策略。

网络安全策略是保障组织网络安全的基础，包括安全检测评估、安全体系结构、安全管理措施和网络安全标准 4 个部分，它们可以组成一个循环系统。安全检测评估随着安全标准的改变而进行，其评估结果又会促进网络体系结构的完善，安全管理措施也会随着其他方面的变化而增强。由于技术的进步及对网络安全要求的提高，又会促使网络标准的改变。它们之间的关系如图 1-6 所示。

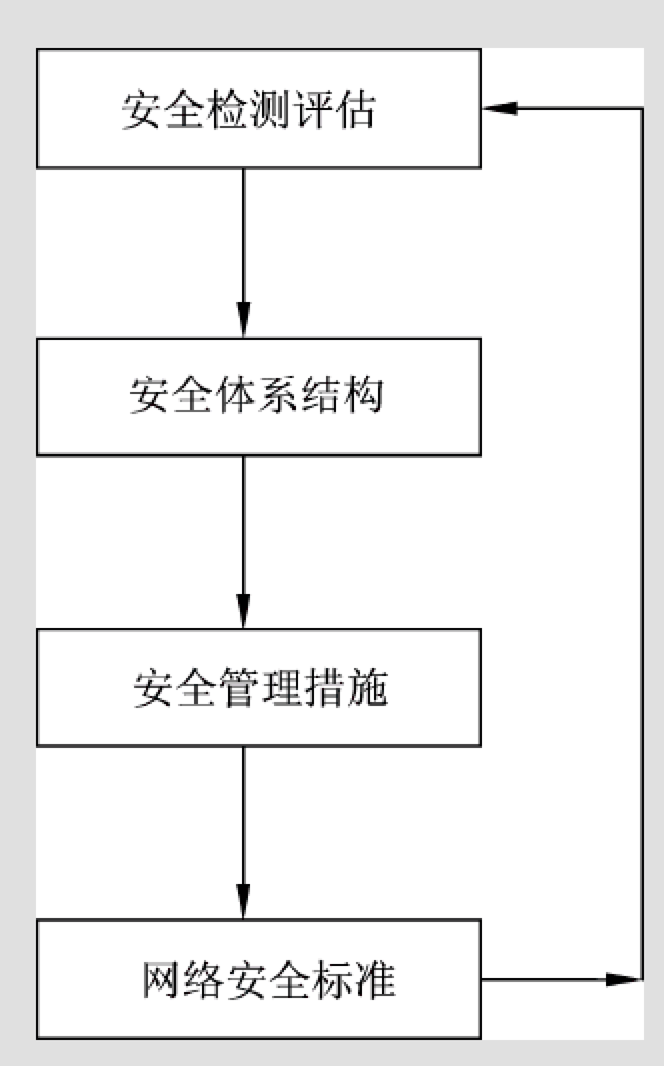


图 1-6　网络安全策略循环系统

1. 安全检测评估

从安全角度看，计算机网络在接入 Internet 前的检测与评估是保障网络安全的重要措施。但大多数组织并没有这样做就把网络接入 Internet。为此介绍一下安全检测评估需要考虑的一些方面。

❑ **网络设备**

重点检测与评估连接不同网段的设备和连接广域网（WAN）的设备，如交换机（Switch）、网桥和路由器等。这些网络设备都有一些基本的安全功能，如密码设置、存取控制列表等，应充分利用这些设备的功能。

❑ **网络操作系统**

网络操作系统是网络信息系统的核心，其安全性占据十分重要的地位。根据美国的“可信计算机系统评估准则”，把计算机系统的安全性从高到低划分为 4 个等级，即 A、B、C、D。DOS、Windows 3.x/95、MacOS 7.1 等系统属于 D 级，即是最不安全的。Windows NT/2000/XP、UNIX、Netware 等则属于 C2 级，一些专用的操作系统可能会达到 B 级。C2 级操作系统已经

有了许多安全特性，但必须对其进行合理的设置和管理，才能使其发挥作用。如在 Windows NT 下设置共享权限时，默认设置是所有用户都是“完全控制（Full Control）”权限，必须对其进行更改。

❑ **数据库及应用软件**

数据库在信息系统中的应用越来越广泛，其重要性也越来越强，如银行用户账号信息、网站的登记用户信息、企业财务信息、企业库存及销售信息等都存在各种数据库中。数据库也具有许多安全特性，如用户的权限设置、数据表的安全性、备份特性等，利用好这些特性也是同网络安全系统很好配合的关键。

❑ **E-mail 系统**

E-mail 的应用范围比数据库的应用还要广泛，而网络中的绝大部分病毒是由 E-mail 传播的，因此，其检测与评估也变得十分重要。

❑ **Web 站点**

许多 Web Server 软件（如 IIS 等）有安全漏洞，相应的产品供应商也在不断解决这些问题。通过检测与评估，进行合理的设置与安全补丁程序，可以把危险尽量降低。

2．安全体系结构

安全体系结构包括物理安全、访问控制、数据保密、数据完整性和路由控制 5 个方面内容。

❑ **物理安全**

物理安全是指在物理介质层次上对存储和传输中的网络信息进行安全保护，是网络信息安全的基本保障。它应从自然灾害（地震、火灾、洪水）、物理损坏（硬盘损坏、设备使用到期、外力损坏）和设备故障（停电断电、电磁干扰）；电磁辐射、乘机而入、痕迹泄露等；操作失误（格式硬盘、线路拆除）、意外疏漏这 3 个方面考虑。

❑ **访问控制**

访问控制将用户和数据进行分类，进而设置用户对数据的访问权限，只有被授权的用户才能访问相应的数据。

❑ **数据保密**

数据保密是保护网络中各系统之间的交换数据，防止数据被截获而造成泄密。它包括连接保密（如对某个连接上的所有用户数据进行保密）、选择字段保密（如对某一协议数据单元中的一部分选择自动进行保密）和信息流保密（对从观察信息流就能获取的信息进行保密）3 个方面。

❑ **数据完整性**

数据完整性保证接收方收到的信息与发送方发送信息的一致性，包括可恢复的完整性、无恢复的完整性、选择字段的完整性。

❑ **路由控制**

在大型网络中，从源节点到目的节点可能会有多条线路，有些线路可能是安全的，但有些则是不安全的。通过路由控制机制，可使信息发送者选择特殊路由，以保证数据的安全性。

3．安全管理措施

网络安全管理既要保证网络用户和网络资源不被非法使用，又要保证网络管理系统本身

不被未经授权的访问。制定合理的安全管理措施是保证网络安全的重要策略之一。它常包括以下几个方面内容。

- **网络设备的安全管理**　包括网络设备的互联、配置更改等原则。
- **软件的安全管理**　它包括软件的使用原则、配置更改原则和权限设置原则等方面。
- **密钥的安全管理**　它包括密钥的生成、检验、分配、保存、更换、注入、销毁等。
- **管理网络的安全管理**　网络管理是集网络维护、运营和信息管理为一体的综合管理系统。主要功能包括性能管理、配置管理、故障管理和计费管理等。
- **安全的行政管理**　安全的行政管理的重点是安全组织的建立、安全人事管理、安全责任与监督等。如在安全组织结构中，应该有一个全面负责的人，负责整个网络信息系统的安全与保密。

4．网络安全标准

网络安全标准是一个具有多学科、综合性、规范性等特点的标准，其目的在于保证网络信息系统的安全运行，保证用户和设备操作人员的人身安全。

一个完整、统一、先进的安全标准体系是十分重要的。通过遵循合适的标准，可以使企业或组织的网络安全有一个较高的起点和较好的规范性，对于网络间的安全互操作也起到关键作用。国内外已制定了许多安全方面的标准，主要分为如下 4 类安全标准。

- **基础类标准**　它包括安全词汇、安全体系结构、安全框架、信息安全技术评价准则等方面内容。
- **物理类标准**　它包括设备电磁泄露规范、保密设备的安全保密规范等。
- **网络类标准**　它包括网络安全协议、网络安全机制、防火墙规范等方面内容。
- **应用类标准**　它包括硬件平台的安全规范、软件应用平台规范、应用业务安全规范、安全工具开发规范、签证机构安全规范等多方面内容。

1.4　网络安全的现状和发展趋势

随着网络应用的日益普及和更为复杂，网络安全事件不断出现，如电脑病毒网络化趋势愈来愈明显，垃圾邮件日益猖獗，黑客攻击成指数增长，利用互联网传播有害信息的手段日益翻新等。网络再给人们带来自由开放的同时，也带来不可忽视的安全风险，目前，网络安全问题越来越成为人们关注的重点。

网络安全问题已成为信息时代人类共同面临的挑战，国内的网络安全问题也日益突出，已成为我国信息产业健康发展必须面对的严重问题。目前，各种网络安全漏洞大量存在和不断被发现；漏洞公布到利用漏洞的攻击代码出现时间缩短至几天甚至一天，使开发、安装相关补丁及采取防范措施的时间压力增加；网络攻击行为日趋复杂，防火墙、入侵监测系统等网络安全设备不能完全阻挡网络安全攻击；黑客攻击目标从单纯追求“荣耀感”向获取实际利益方向转移；针对手机等无线终端的网络攻击也在进一步发展；随着网络共享软件、群组交互通信、地址转移、加密代理、信件自收发、无界浏览器、动态网络等新型技术的不断开发和应用，传统的网络安全监管手段和技术实施措施难以有效发挥。

正是因为网络安全威胁无处不在，才使得安全这个字眼被越来越多地提及。由于网络规模的不断扩张以及各种应用类型的不断融合，信息社会正处于一个极大繁荣而又不受控制的“喧嚣”阶段。特别是无线技术的迅猛发展，加速了网络边界从人们视线中消失的速度。而通信协议和网络应用的发展在引领人们跨越交流障碍的同时，也为各种安全威胁提供了“机会”。

目前威胁主流操作系统的安全漏洞已经数以千计。即使在一个小型的企业网中，也难以对每个可能发生安全问题的地方进行监控，而在浩瀚的互联网世界，更是有无以计数的危险。

因此，不管是企业还是个人用户在使用信息产品和网络服务时，都开始对安全问题表现出不同程度的担忧，安全性及安全功能已经成为焦点。未来网络安全将呈现以下发展趋势。

1. 安全需求多样化

随着我国信息化建设的推进，用户对于安全保障的要求越来越高，对网络安全的需求越来越大。安全需求将从单一安全产品发展到综合防御体系，从某一点的安全建设过渡到整个安全体系的建设。网络与信息安全部署的重点开始由“网络安全”向“应用安全”嬗变，应用安全和安全管理会逐渐热起来。

2. 技术发展两极分化

两极分化包括专一和融合两个方面。诸如防火墙、（入侵检测系统）IDS、内容管理等产品方案越做越专，这是因为在安全需求较高的电信行业须应对复杂多变的安全威胁。同时，融合也是一种趋势，基本的防火墙功能也被集成到了越来越多的网络设备当中。路由器和交换机设备开始整合防火墙过滤功能。在新出现的一些 64 位计算机主板上，也在芯片组中提供了防火墙功能。

除了防火墙功能之外，还有很多安全功能被整合进了各种产品中。在软件领域，安全功能除了在软件系统中被越来越多地考虑之外，大量进行网络管理的软件都增加了防范恶意程序及行为的机制。

3. 安全管理体系化

俗话说，“三分技术，七分管理”，管理作为网络与信息安全保障的重要基础，一直倍受重视。在国家宏观管理方面，我国将在“积极防御、综合防范”的管理方针指导下，逐步建立并完善国家信息安全管理保障体系，进一步完善国家互联网应急响应管理体系的建设，加快网络与信息安全标准化的制定和实施工作，加强电信安全监管和信息安全等级保护工作，对电信设备的安全性和信息安全专用产品实行强制性认证等。

在网络信息系统微观管理方面，网络与信息安全管理正逐渐成为企业管理越来越关键的一部分，越来越多的企业将在近年内逐步建立自身的信息安全管理体系（ISMS）。

4. 集团化、产业化的趋势

- ❑ 产业链：病毒木马编写者－专业盗号人员－销售渠道－专业玩家。
- ❑ 病毒不再安于破坏系统，销毁数据，而更关注财产和隐私。
- ❑ 电子商务成为热点，针对网络银行的攻击也更加明显。
- ❑ 病毒会更加盯紧在线交易环节，从早期的虚拟价值盗窃转向直接金融犯罪。

5．“黑客”逐渐变成犯罪职业

财富的诱惑，使得黑客对网络的袭击不再是一种个人兴趣，而是变成一种有组织的、利益驱使的职业犯罪。例如，使用拒绝服务进行的敲诈勒索和“网络钓鱼”等。

6．恶意软件的转型

我国仍然是恶意软件最多的国家。恶意软件在行为上将有所改观，病毒化特征削弱，但手段更“高明”，包含更多的钓鱼欺骗元素。

7．网页挂马危害继续延续

网页挂马成为网络木马传播的“帮凶”，使得服务器端系统资源和流量带宽资源大量损失。另外，客户端的用户个人隐私也将受到威胁。

8．利用应用软件漏洞的攻击将更为迅猛

由于当前应用软件在开发中都存在这样或那样的不足，这些不足常被入侵者发现并加以利用，新的漏洞出现要比设备制造商修补的速度更快。另外，在一些嵌入式系统中的漏洞难以修补。

9．Web 2.0 的产品将受到挑战

Web 2.0 是以网络相簿（Flickr）、克雷格列表（Craigslist）、人际关系网（Linkedin）、交友网站（Friendster）等网站为代表，以博客（Blog）、标签（TAG）、社会性网络服务（Social Networking Services，SNS）、简易信息集合（RSS）、多人协作写作工具（Wiki）等应用为核心，依据六度分隔、可扩展标示语言（Xml）、创建交互式 Web 应用程序而无需牺牲浏览器兼容性的流行方法（Ajax）等新理论和技术实现的互联网新一代模式。

然而，以博客、论坛为首的 Web 2.0 产品将成为病毒和网络钓鱼的首要攻击目标，社区网站上带有社会工程学性质的欺骗往往超过安全软件所保护的范畴。

另外，自动邮件发送工具日趋成熟，垃圾邮件制造者正在将目标转向音频和视频垃圾邮件。

第2章 计算机病毒

计算机病毒对计算机系统及网络所产生的破坏效应，使人们清醒地认识到它所带来的危害。目前，每年的新病毒数量都是呈指数级增长，而且由于近几年传输媒介的改变和因特网的大面积普及，导致计算机病毒感染的对象也开始由工作站向网络设备（代理、防护和服务器设置等）转变，病毒的类型也由文件型向网络蠕虫型转变。如今，世界上很多国家的科研机构都在对病毒的现状和防护进行深入研究。

计算机病毒不仅能够破坏用户数据、盗取用户隐私数据甚至会使个人或者企业甚至国家遭受经济损失。因此，本章从计算机病毒的起源、发展、定义和结构以及常见计算机病毒类型、计算机病毒的危害及防范措施方面进行学习，使用户全面了解计算机病毒，避免或者减小病毒所造成的破坏。

本章学习要点：

- 了解计算机病毒的起源及发展过程
- 了解计算机病毒的定义、命名规则及分类
- 了解计算机病毒的结构
- 熟悉计算机病毒的特征及表现
- 熟悉常见的计算机病毒类型

2.1 计算机病毒概述

众所周知，对网络安全最具威胁的因素之一就是计算机病毒。计算机病毒可以感染健康的程序，并在短时间内感染其他计算机。计算机病毒就是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活的具有对计算机资源进行破坏作用的一组程序或指令集合。

2.1.1 计算机病毒的起源

目前，关于计算机病毒的起源还没有一个确切的说法。尽管如此，对于计算机病毒的发源地，人们都一致认为是在美国。

1. 科学幻想起源说

1977 年，美国科普作家托马斯·丁·雷恩推出轰动一时的《Ado1escence of P-1》一书。

书中构思了一种能够自我复制，利用信息通道传播的计算机程序，并称之为计算机病毒。这是世界上第一个幻想出来的计算机病毒。人类社会有许多现行的科学技术，都是在先有幻想之后才成为现实的。因此，不能否认这本书的问世对计算机病毒的产生所起的作用。

2．恶作剧起源说

恶作剧者大多是那些对计算机知识和技术均有兴趣的人，并且特别热衷于别人认为是不可能做成的事情，因为他们认为世上没有做不成的事。这些人或是要显示一下自己在计算机知识方面的天资，或是要报复一下别人或单位。前者是无恶意的，所编写的病毒也大多不是恶意的，只是和对方开个玩笑，显示一下自己的才能以达到炫耀的目的。虽然计算机病毒的起源是否归结于恶作剧者还不能确定，但可以肯定，世界上流行的许多计算机病毒都是恶作剧者的产物。

3．游戏程序起源说

在 20 世纪 70 年代，计算机在人们的生活中还没有得到普及，美国贝尔实验室的计算机程序员为了娱乐，在自己实验室的计算机上编制吃掉对方程序的程序，看谁先把对方的程序吃光，有人认为这是世界上第一个计算机病毒，但这只是一个猜测。

4．软件商保护软件起源说

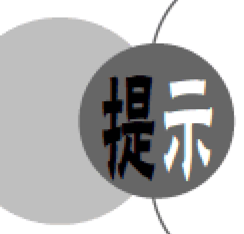
计算机软件是一种知识密集型的高科技产品，由于人们对于软件资源的保护不尽合理，这就使得许多合法的软件被非法复制的现象极为平常，从而使得软件制造商的利益受到了严重的侵害。因此，软件制造商为了处罚那些非法复制者，而在软件产品中加入病毒程序并由一定条件触发传染。例如，Pakistani Brain 病毒在一定程度上就证实了这种说法。该病毒是巴基斯坦的两兄弟为了追踪非法复制其软件的用户而编制的，它只是修改磁盘卷标，把卷标改为 Brain 以便识别。也正因为如此，当计算机病毒出现之后，有人认为这是软件制造商为了保护自己的软件不被非法复制而导致的结果。

2.1.2　计算机病毒的发展过程

计算机病毒是一段附着在其他程序上的，可以实现自我繁殖的程序代码。自 1985 年在美国被当众证明其存在性之后，计算机病毒技术得到了突飞猛进的发展。通常，计算机病毒的发展是相对于计算机操作系统来说的。据此，计算机病毒经历了如下几个发展阶段。

1．DOS 引导阶段

最早在 1987 年，计算机病毒主要是引导型病毒，具有代表性的是“小球”、2708 病毒和“石头”病毒等。由于在该时期的电脑硬件较少，功能简单，经常使用软盘启动和用软盘在计算机之间传递文件。而引导型病毒正是利用了软盘的启动原理来工作，它能够修改系统引导扇区，在计算机启动时首先取得控制权，减少系统内存，修改磁盘读写中断，在系统存取磁盘时进行传播。



这些病毒也是随着软盘悄悄地由美国进入我国，并在人们懵懂之间在大型企业和研究所广为传播。直到病毒发作，人们才猛然惊醒。目前认为，小球病毒是国内发现的第一个计算机病毒。

2. DOS可执行阶段

在1989年，当时家庭计算机尚未普及，因此各研究所和高等院校的计算机密集地区成了计算机病毒的重灾区，而且往往是多种不同病毒的反复交叉感染。此时的病毒称为可执行文件型病毒，它们利用DOS系统加载执行文件的机制工作，如“耶路撒冷”、“星期天”等病毒。可执行型病毒的代码在系统执行文件时取得控制权，修改DOS中断，在系统调用时进行传染，并将自己附加在可执行文件中，使文件长度增加。到了1990年，这种病毒发展成为复合型病毒，可同时感染COM和EXE文件。

但是，随着软件技术的发展，人们逐渐了解和掌握计算机病毒，计算机病毒也不再那么神秘。人们逐渐研究出了反病毒软件，如SCAN、TBAV等。

3. 批处理阶段

1992年，伴随型病毒出现，利用DOS加载文件的优先顺序进行工作。它感染EXE文件的同时会生成一个和EXE同名而扩展名为COM的伴随体；相反，当感染COM文件时，改为原来的COM文件为同名的EXE文件，再产生一个原名的伴随体，文件扩展名为COM。这样，在DOS加载文件时，总是先加载扩展名为COM的文件，病毒文件会取得控制权，优先执行自己的代码。具有代表性的是“金蝉”病毒。

伴随型病毒并不改变原来文件的内容、日期及属性，解除病毒时只要将其伴随体删除即可。其典型代表是“海盗旗”病毒，它在得到执行时，会询问用户名和口令，然后返回一个出错信息，并将自身删除。

4. 多形阶段

1994年，汇编语言得到了快速的发展。一种功能可以通过汇编语言用不同的方式来实现，这些方式的组合使一段看似随机的代码产生相同的运算结果。例如，典型的变形病毒“幽灵病毒”就是利用了这个特点，每感染一次就产生不同的代码。“一半”病毒就是产生一段有上亿种可能的解码运算程序，病毒体被隐藏在解码前的数据中，查解这类病毒就必须能对这段数据进行解码，因此加大了查毒的难度。

变形病毒是一种综合性病毒，它既能感染引导区，又能感染程序区，多数具有解码算法，一种病毒往往要两段以上的子程序方能解除。

5. 变种阶段

1995年，在汇编语言中，一些数据的运算放在不同的通用寄存器中可运算出同样的结果，随机插入一些空操作和无关命令，也不影响运算的结果。这样，某些解码算法可以由生成器生成不同的变种。例如，“病毒制造机”VCL，它可以在瞬间制造出成千上万种不同的病毒，

查解时不能使用传统的特征码识别法，而需要在宏观上分析命令，解码后方可查解病毒，大大提高了复杂程度。

6．网络、蠕虫阶段

蠕虫是无须计算机使用者干预即可运行的独立程序，通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行蠕动。1995 年，随着网络的普及，病毒开始利用网络进行传播，它们只是以上几代病毒的改进。在 Windows 操作系统中，"蠕虫"是典型的代表，它不占用除内存外的任何资源，不修改磁盘文件，利用网络功能搜索网络地址进行传播，有时也存在网络服务器和启动文件中。

7．Windows 病毒阶段

1996 年，随着微软 Windows 和 Windows 95 操作系统的日益普及，利用 Windows 进行工作的病毒开始发展，它们修改（NE，PE）文件，典型的代表是 DS.3873 病毒，这类病毒利用保护模式和 API 调用接口进行工作，清除的方法也比较复杂。

8．宏病毒阶段

1996 年以后，随着 MS Office 功能的增强及流行，使用 Word 宏语言也可以编制病毒，这种病毒使用 VB Script 语言，编写容易，感染 Word 文档文件。在 Excel 和 AmiPro 出现的相同工作机制的病毒也属于此类。

9．互联网病毒阶段

1997 年以后，随着因特网的发展，各种病毒也开始利用因特网进行传播，携带病毒的数据包和邮件越来越多，如果用户不小心打开这些邮件或登录带有病毒的网页，计算机就有可能中毒。典型的有"尼姆达"、"欢乐时光"和"欢乐谷"等病毒。

2003 年，"2003 蠕虫王"病毒在亚洲、美洲、澳大利亚等地迅速传播，造成了全球性的网络灾害。其中受害最严重的无疑是美国和韩国这两个因特网发达的国家。韩国 70%的网络服务器处于瘫痪状态，网络连接的成功率低于 10%，整个网络速度极慢。美国不仅公众网络受到了破坏性的攻击，而且连银行网络系统也遭到了破坏，全国 1.3 万台的自动取款机处于瘫痪状态。

2004 年是"蠕虫"泛滥的一年，根据中国计算机病毒应急中心的调查显示，2004 年 10 大流行病毒都是蠕虫病毒，它们分别是网络天空（Worm.Netsky）、高波（Worm.Agobot）、爱情后门（Worm.Lovgate）、震荡波（Worm.Sasser）、SCO 炸弹（Worm.Novarg）、冲击波（Worm.Blaster）、恶鹰（Worm.Bbeagle）、小邮差（Worm.Mimail）、求职信（Worm.Klez）、大无极（Worm.SoBig）。

2005～2008 年是木马流行的年代。2008 年上半年，江民反病毒中心共截获新病毒 206439 种，另据江民病毒预警中心不完全统计，1～6 月全国共有 9871681 台计算机感染了病毒。其中感染木马病毒的计算机 7749269 台，占病毒感染计算机总数的 78.5%，比去年同期增长 11 个百分点；感染广告程序的计算机 3849955 台，占病毒感染计算机总数的 3.9%；感染后门程序的计算机 4540973 台，占病毒感染计算机总数的 4.6%；感染蠕虫病毒的计算机 2764070 台，

占病毒感染计算机总数的 2.8%；监测发现漏洞攻击代码感染的计算机 1184601 台，占病毒感染计算机总数的 1.2%；感染脚本病毒的计算机 888451 台，占病毒感染计算机总数的 0.9%。由此可见，木马将是未来几年的病毒主流。

表 2-1　近年来几种病毒带来的巨大危害

时间	攻击行为发起者	受害计算机数目	损失金额（美元）
2006	木马和恶意软件	（破坏程度不可估计）	（破坏程度不可估计）
2005	木马	（破坏程度不可估计）	（破坏程度不可估计）
2004	Worm_Sasser（震荡波）	（破坏程度不可估计）	（破坏程度不可估计）
2003	Worm_Blast（冲击波）	超过 140 万台	（破坏程度不可估计）
2003	SQL Slammer	超过 20 万台	9.5 亿至 12 亿
2002	Klez	超过 600 万台	90 亿
2001	RedCode	超过 100 万台	26 亿
2001	NIMDA	超过 800 万台	60 亿
2000	Love Letter	（破坏程度不可估计）	88 亿
1999	CIH	超过 6000 万台	近 100 亿

如今，计算机病毒变得更加活跃，木马、蠕虫、后门等病毒层出不穷，甚至出现了 2006 年炒得火热的流氓软件。自 2000 年以来，由于病毒的基本技术和原理被越来越多的人所掌握，新病毒的出现以及原有病毒的变种层出不穷，病毒的增长速度超过了以往的任何时期。

科技的进步，在带来技术飞跃的同时也带来了新的研究课题。计算机技术被迅速掌握的同时，出现了大批以病毒盈利的程序开发者。有专家总结，病毒发展到今天，开发者已经很少或不再以炫耀自己的技术为主要目的，更多地把矛头对准网络用户的信息，网络犯罪事件大大增加。幸好国内外各大厂商已经十分重视网络安全问题，纷纷出台了不同的安全防范措施。

2.1.3　计算机病毒的定义

计算机中的病毒是一个程序，一段可执行代码。与生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

除复制能力外，某些计算机病毒还有其他一些共同特性：一个被污染的程序能够传送病毒载体。当看到病毒载体似乎仅仅表现在文字和图像上时，它们可能已毁坏了文件、再格式化硬盘驱动或引发其他类型的灾害。若病毒并不寄生于一个污染程序，它仍然能通过占据存储空间带来麻烦，并降低计算机的全部性能。

可以从不同角度给计算机病毒进行定义。其中，一种定义是通过磁盘、磁带和网络等作为传输媒介进行传播扩散，能“传染”其他程序的程序；另一种是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。

另外，在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒是指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我

复制的一组计算机指令或者程序代码”。

还有一种定义是：一种人为制造的程序，通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存）或程序里。当某种条件或时机成熟时，它会自我复制并传播，使计算机的资源受到不同程度的破坏。这些说法在某种意义上借用了生物病毒的概念，计算机病毒同生物病毒的相似之处是计算机病毒能够入侵计算机系统和网络，危害正常工作的“病原体”（是指计算机中存放的数据或系统本身），能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。

2.1.4　计算机病毒的分类

从第一个病毒问世以来，病毒的种类多得已经让人们难以准确统计。时至今日，病毒的数量仍在不断增加。据国外统计，计算机病毒数量正在以 10 种每周的速度递增，另据我国公安部统计，国内以 4～6 种每月的速度在递增。

计算机病毒的分类方法有很多种，对于同一种病毒可能有多种不同的分类分法，主要有如下几种分类方法。

1．按照传播介质进行分类

从计算机病毒使用的传播介质来分类，病毒可分为单机病毒和网络病毒两种类型。

- **单机病毒**

单机病毒的载体是磁盘，一般情况下，病毒从 USB 盘、移动硬盘传入硬盘，感染系统，然后再传染其他 USB 盘和移动硬盘，接着传染其他系统，如 CIH 病毒。

- **网络病毒**

网络病毒的传播介质不再是移动式存储载体，而是网络通道，这种病毒的传染能力更强，破坏力更大，如“尼姆达”病毒。

另外，当前的病毒通常是以网络传播的方式感染其他系统。病毒也可能综合了其他病毒的若干特征，这样的病毒称为混合型病毒。

混合型病毒就是指以上几种病毒的混合。混合型病毒是为了综合利用以上几种病毒的传染渠道进行破坏。混合型病毒不仅传染可执行文件而且还传染硬盘主引导扇区，被这种病毒传染的计算机不能通过使用 FORMAT 命令格式化硬盘来清除。

2．按照计算机病毒的破坏性质进行分类

按照病毒对计算机造成破坏的性质进行划分，可以将病毒分为如下两种类型。

- **良性病毒**

良性病毒是指不包含对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据。有些只是表现为恶作剧。这类病毒取得系统控制权后，会导致整个系统的运行效率降低，系统可用内存总数减少，使某些应用程序暂时无法执行。

- **恶性病毒**

恶性病毒又称逻辑炸弹或定时炸弹，是指在代码中包含损伤和破坏计算机系统的操作，

在其传染或发作时会对系统产生直接的破坏作用。这类病毒有很多，如米开朗基罗病毒。当米氏病毒发作时，硬盘的前 17 个扇区将被彻底破坏，使整个硬盘上的数据无法恢复，造成的损失是无法挽回的。有的病毒甚至还会对硬盘做格式化等破坏操作。

3. 按照计算机病毒的链接方式进行分类

根据计算机病毒的链接方式，可以将其划分为如下几种不同类型。

❑ **源码型病毒**

这种病毒主要攻击高级语言编写的程序，该病毒在高级语言所编写的程序编译前插入到原程序中，经编译成为合法程序的一部分。

❑ **嵌入型病毒**

这种病毒是将自身嵌入到现有程序中，把病毒的主体程序与其攻击的对象以插入的方式链接。

❑ **外壳型病毒**

这种病毒将其自身包围在被入侵的程序周围，对原来的程序不做修改。这种病毒最为常见，易于编写，也易于发现，一般测试文件的大小即可查出。

❑ **操作系统型病毒**

这种病毒用它自己的程序代码加入或取代部分操作系统代码进行工作，具有很强的破坏力，可以使整个系统瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。

4. 按照计算机病毒的寄生部位或传染对象进行分类

传染性是计算机病毒的本质属性，根据寄生部位或传染对象进行划分，也就是根据计算机病毒的传染方式进行划分，包括如下几种类型。

❑ **磁盘引导型病毒**

引导型病毒又称引导扇区病毒，驻留在计算机硬盘上的特定区域，这个区域只在启动时被计算机读取、执行。

磁盘引导区传染的病毒主要是用病毒的全部或部分逻辑取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其他地方。由于引导区是磁盘能正常使用的先决条件，因此，这种病毒在运行的一开始（如系统启动时）就能获得控制权，其传染性较大。由于在磁盘的引导区内存储着需要使用的重要信息，因此，如果对磁盘上被移走的正常引导记录不进行保护，在运行过程中就会导致引导记录的破坏。例如，“大麻”和“小球”病毒就属于引导区传染的计算机病毒。

❑ **操作系统型病毒**

操作系统是计算机应用程序得以运行的支持环境，它由.sys、.exe 和.dll 等许多可执行的程序及程序模块构成。操作系统型病毒就是利用操作系统中的一些程序及程序模块寄生并传染。通常，这类病毒成为操作系统的一部分，只要计算机开始工作，病毒就处在随时被触发的状态。而操作系统的开放性和不完善性给这类病毒出现的可能性与传染性提供了方便。例如，“黑色星期五”就是这样的病毒。

❑ **感染可执行程序的病毒**

通过感染可执行程序进行传染的病毒通常寄生在可执行程序中，一旦程序被执行病毒就

会被激活，病毒程序首先被执行，并将自身驻留内存，然后设置触发条件进行传染。

❑ 感染带有宏的文档

随着微软公司 Office 软件的广泛使用和计算机网络尤其是 Internet 的推广和普及，病毒家族又出现了一个新成员——宏病毒。宏病毒是一种寄存于文档或模板的宏中的计算机病毒。一旦打开这样的文档，宏病毒就会被激活并转移到计算机上，且驻留在 Normal 模板中。此后，所有自动保存的文档都会感染上这种宏病毒，而且，如果其他用户打开了已感染病毒的文档，宏病毒又会转移到该用户的计算机中。

在该分类方法中，除磁盘引导型病毒外，其余 3 种病毒的分类又都属于文件型病毒。文件型病毒又叫寄生型病毒，这类病毒把自身附着在可执行文件上，是一类最常见，也是讨论得最多的病毒。这样的病毒通常驻留在内存里，等待用户运行其他程序，把这当作触发它的事件，触发后感染新打开的程序。所以，它们的复制很简单，只需要通过计算机的正常使用就可进行。

5. 按照病毒特有的算法进行分类

编制者在制造病毒时，用到的算法不止一种，因此根据病毒特有的算法，可以将其划分为如下几种类型。

❑ 伴随型病毒

该类型病毒并不改变文件本身，它们根据自身算法产生 EXE 文件的伴随体，具有同样的名字和不同的扩展名（COM），例如，XCOPY.EXE 的伴随体是 XCOPY.COM。病毒把自身写入 COM 文件并不改变 EXE 文件，当 DOS 加载文件时，伴随体优先被执行到，再由伴随体加载执行原来的 EXE 文件。

❑ “蠕虫”型病毒

该类型病毒通过计算机网络进行传播，不改变文件和资料信息，利用网络从一台计算机的内存传播到其他计算机的内存。它能够计算网络地址，将自身的病毒通过网络进行传输。有时它们在系统中存在，但一般除了内存不占用其他资源。

❑ 寄生型病毒

在该分类方法中，除了伴随和“蠕虫”型病毒外，其他病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播。

❑ 诡秘型病毒

它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技术。利用 DOS 空闲的数据区进行工作。

❑ 变型病毒（幽灵病毒）

这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般由一段混有无关指令的解码算法和被修改过的病毒体组成。

2.1.5　计算机病毒的命名

反病毒公司为了方便管理，通常会按照病毒的特性，将病毒进行分类命名。虽然，每个反病毒公司的命名规则各不相同，但大体上都是采用一种统一的命名方法来命名。一般格式

为：<病毒前缀>.<病毒名>.<病毒后缀>。在该格式中，对于各部分有如下解释。

❑ **病毒前缀**

病毒前缀指一个病毒的种类，用来区别病毒的种族分类。不同种类的病毒，其前缀也不同。例如，常见的木马病毒的前缀是 Trojan，蠕虫病毒的前缀是 Worm，黑客病毒前缀名一般为 Hack，宏病毒的前缀是 Macro，脚本病毒的前缀是 Script，系统病毒的前缀为 Win32、PE、Win95、W32、W95 等，捆绑机病毒的前缀是 Binder，后门病毒的前缀为 Backdoor 等。

❑ **病毒名**

病毒名指一个病毒的名称，用来区别和标识病毒家族。如著名的 CIH 病毒的家族名都是统一的 CIH，"振荡波"蠕虫病毒的家族名是 Sasser。

❑ **病毒后缀**

病毒后缀指一个病毒的变种特征，用来区别具体某个家族病毒的某个变种。一般采用英文中的 26 个字母来表示，如 Worm.Sasser.B 就是指振荡波蠕虫病毒的变种 B，因此一般称为"振荡波 B 变种"或者"振荡波变种 B"。如果该病毒变种非常多，可以采用数字与字母混合作为变种标识。

2.1.6 网管心得——计算机病毒的结构

计算机病毒可能是用不同的编程语言所编写，也可能运行于不同的操作系统，但其逻辑结构通常是不变的，包括感染模块、触发模块、破坏模块和引导模块 4 个组成部分。

1. 感染模块

感染模块是病毒的传染部分，是病毒程序的一个重要组成部分，主要负责病毒的传染和扩散。但是，为了避免病毒重复感染一个文件、一个扇区，病毒要在病毒数据中加一个标志，如 CIH 病毒的感染标志是加了"CIH"字符串。对于以独立文件方式存在的病毒，如冲击波病毒，为了避免多个病毒进程同时运行，使用函数 CreateMutex 建立了一个互斥变量 BILLY，病毒启动时首先检测有无该变量存在，存在则说明病毒程序已经运行，这样就保证了内存中只有一份病毒文件生成的进程。

病毒的传染性是病毒赖以生存繁殖的条件，如果计算机病毒没有传播渠道，则其破坏性小，扩散面窄，难以造成大面积流行。

病毒传染的条件包括静态和动态两种。其中，静态传染是指被动传染，如用户在进行备份磁盘或文件时，把一个病毒由一个载体复制到另一个载体上，或者是通过网络上的信息传递，把一个病毒程序从一方传递到另一方；动态传染是指主动传染，以计算机系统的运行及病毒程序处于激活状态为先决条件。在病毒处于激活的状态下，只要传染条件满足，病毒程序就能够主动地把病毒自身传染给另一个载体或另一个系统。

2. 触发模块

触发模块的目的是调节病毒的攻击性和潜伏性之间的平衡。因为，病毒大范围的感染、频繁的破坏行为可能给用户以重创，但是，它们总是使系统或多或少地出现异常，因此容易使病毒暴露。不破坏、不感染又会使得病毒失去其特性，而可触发性是病毒的攻击性和潜伏性之间的调整杠杆，可以控制病毒的感染和破坏的频度，兼顾病毒的杀伤力和潜伏性。

计算机病毒在传染和破坏之前，往往要判断某些条件是否满足，满足则传染或者发作，否则不传染或不发作或只传染不发作，这个条件就是计算机病毒的触发条件。该条件是预先由病毒编制者设置的，通过触发模块能够判断触发条件是否满足，并根据判断结果来控制病毒的传染和破坏动作。

病毒采用的触发条件花样繁多，从中可以看出病毒作者对系统的了解程度及其丰富的想象力和创造力。病毒采用的触发条件主要包括如下几种。

- **日期触发** 许多病毒采用日期来做触发条件。日期触发包括特定日期触发、月份触发、前半年或后半年触发等。
- **时间触发** 时间触发包括特定的时间触发、染毒后累计工作时间触发、文件最后写入时间触发等。
- **启动触发** 启动触发是指病毒对计算机的启动次数进行计数，并将此值作为触发条件。
- **键盘触发** 有些病毒监视用户敲打键盘的动作，当发现病毒预定的键入时，病毒被激活并进行某些特定的操作。键盘触发包括击键次数触发、组合键触发、热启动触发等。
- **感染触发** 感染触发以运行感染文件的个数、感染序数、感染磁盘数、感染失败等为触发条件。
- **操作系统触发** 某些病毒攻击特定的操作系统，特定的版本或特定的语言版本等。
- **访问磁盘次数触发** 访问磁盘次数触发是指病毒对磁盘的 I/O 访问次数进行计数，以预定的次数作为触发条件。
- **调用中断功能/API 函数触发** 病毒对中断调用或函数调用的次数进行计数，以预定的次数作为触发条件。
- **CPU 型号/主板型号触发** 病毒能识别运行操作系统环境下的 CPU 型号/主板型号，以指定的 CPU 型号/主板型号作为触发条件，这种病毒的触发方式奇特罕见。

3. 破坏模块

破坏模块是病毒程序中最为关键的部分，负责病毒的破坏工作，其破坏对象通常包括系统数据区、文件、内存、系统运行速度、磁盘、CMOS、主板和网络等。



在计算机领域，CMOS 通常指保存计算机基本启动信息（如日期、时间、启动设置等）的芯片。

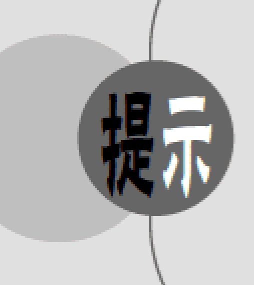
4. 引导模块

病毒程序运行时，首先运行的是病毒的引导模块，它主要负责操作系统环境检测，感染标志检测，分配内存，将自己读到内存，设置病毒触发条件，检查是否满足触发条件等。例如，CIH 病毒首先检测系统是否为 Windows 95/98，否则病毒程序退出。

计算机病毒实际上是一种特殊的程序，程序必然要存储在磁盘上，但是病毒程序为了进行自身的主动传播，必须使自身寄生在可以获取执行权的对象上。

病毒的寄生对象有两种：一种是寄生在磁盘引导扇区；另一种是寄生在可执行文件（.exe 或.com）中。这是由于不论是磁盘引导扇区还是可执行文件，它们都有获取执行权的可能，

这样病毒程序寄生在它们上面，就可以在一定条件下获得执行权，从而使病毒得以进入计算机系统，并处于激活状态，然后进行病毒的动态传播和破坏活动。



.com 文件是 DOS 系统下一种最简单的以 COM（Copy Of Memory）结尾的可执行文件。COM 文件最大为 64KB，内含 16 位程序的二进制代码映像，没有重定位信息，也就是说为了运行程序能够准确地执行处理器指令和内存中的数据，DOS 通过直接将该映像从文件复制到内存以加载 COM 程序，系统不需要做重定位工作。

计算机病毒的寄生方式有两种：一种是采用替代法；另一种是采用链接法。其中，替代法是指病毒程序用自己的部分或全部指令代码，替代磁盘引导扇区或文件中的全部或部分内容；链接法是指病毒程序将自身代码作为正常程序的一部分与原有正常程序链接在一起，病毒链接的位置可能在正常程序的首部、尾部或中间。寄生在磁盘引导扇区的病毒一般采取替代法，而寄生在可执行文件中的病毒一般采用链接法。

通常计算机病毒的引导过程包括以下 3 个方面。

❑ **驻留内存**

病毒若要发挥其破坏作用，一般要驻留内存。为此就必须开辟所用内存空间或覆盖系统占用的部分内存空间。但是，也有一些病毒不驻留内存，如 Taiwan（台湾）病毒（感染 COM、EXE 文件，发作时显示图像或动画）。

❑ **窃取系统控制权**

在病毒程序驻留内存后，必须使有关部分取代或扩充系统的原有功能，并窃取系统的控制权。此后病毒程序依据其设计思想，隐蔽自己，等待时机，在条件成熟时，再进行传染和破坏。

❑ **恢复系统功能**

病毒为隐蔽自己，驻留内存后还要恢复系统，使系统不会死机，只有这样才能等待时机成熟后，进行感染和破坏。

另外，某些病毒在加载之前进行动态反跟踪和病毒体解密。对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占据原系统引导程序的位置，并把原系统引导程序搬移到一个特定的位置。这样系统一启动，病毒引导模块就会自动地装入内存并获得执行权，然后该引导程序负责将病毒程序的传染模块和破坏模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对该两个模块设定某种激活方式，使之在适当的时候获得执行权。处理完这些工作后，病毒引导模块将系统引导模块装入内存，使系统在带毒状态下运行。

对于寄生在可执行文件中的病毒来说，病毒程序一般通过修改原有可执行文件，使该文件执行首先转入病毒程序引导模块，该引导模块也完成把病毒程序的其他两个模块驻留内存及初始化的工作，然后把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。

2.2 计算机病毒的危害

在计算机病毒出现的初期，计算机病毒的危害，往往注重于病毒对信息系统的直接破坏

作用，比如格式化硬盘、删除文件数据等，并以此来区分恶性病毒和良性病毒。但是，这些只是病毒劣迹的一部分，随着计算机应用的发展，人们深刻地认识到凡是病毒都可能对计算机信息系统造成严重的破坏。

2.2.1　计算机病毒的表现

计算机病毒是一种可存储的、可执行的非法程序，其最终目的是破坏计算机系统的正常运行，待时机成熟一定会表现它的存在。因此，计算机在受到病毒感染后，会表现出不同的症状。下面将一些经常碰到的表现症状作一简单介绍，以供用户参考判断当自己的计算机出现问题时是不是由病毒造成的。

1. 计算机无法正常启动

当计算机通电后，根本不能启动，或者可以启动，但所需要的时间比原来的启动时间变长了。有时会突然出现黑屏现象。

2. 运行速度降低

病毒可能会修改进程内存数据、插入进程空间、引起某些进程溢出、造成某些服务程序崩溃等。病毒激活后，其运行将占用系统时间，造成其他程序运行速度变慢。

另外，如果发现在运行某个程序时，读取数据的时间比原来长，存储文件或读取文件的时间都明显增加，那就可能是由于病毒造成的。

3. 内存空间不足

内存是计算机的重要资源，也是病毒的攻击目标。病毒额外地占用和消耗系统的内存资源，使内存空间变小甚至变为“0”，从而导致其他程序无法正常使用内存。

4. 文件内容和长度有所改变

一个文件存入磁盘后，本来它的长度和内容都不会改变，但是由于病毒的干扰，文件长度可能改变，文件也可能出现乱码。有时文件内容无法显示或显示后又突然消失。

5. 经常出现“死机”现象

在计算机中，正常的操作是不会造成死机现象的，即使是初学者，命令输入不对也不会死机。如果机器经常死机，那可能是系统被病毒感染了。

6. 外部设备工作异常

由于外部设备受系统的控制，如果计算机中有病毒，外部设备在工作时可能会出现一些异常情况。例如，干扰打印机，使之产生假报警、间断性打印、更换字符等。

另外，有的病毒还会使计算机的喇叭发出响声。有的病毒设计者让病毒演奏旋律优美的世界名曲，在高雅的曲调中去杀戮人们的信息财富，如演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、嘀嗒声等。

7. 扰乱屏幕显示

病毒扰乱屏幕显示的方式很多，如字符跌落、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写等。

2.2.2 计算机病毒特征

计算机病毒是人为编写的，具有自我复制能力，是未经用户允许而执行的代码。

一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务，其目的对用户是可见的、透明的。而计算机病毒具有正常程序的一切特征，它隐藏在正常程序中，当用户调用正常程序时，它窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的和未经用户允许的。通常，病毒包括如下主要特征。

❑ **传染性**

一般情况下，正常的计算机程序不会将自身的代码强行连接到其他程序上面。而病毒却能够使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可以通过各种可能的渠道（如软盘、光盘和计算机网络）去传染其他计算机。当用户在一台计算机上发现了病毒时，则在这台计算机上使用过的软盘或光盘也已经感染上了病毒，而与这台计算机联网的其他计算机或许也被该病毒感染了。是否具有传染性是判别一段程序是否为计算机病毒的最重要条件。

❑ **隐蔽性**

病毒一般是具有很高编程技巧、短小精悍的一段程序，通常潜入在正常程序或磁盘中。病毒程序与正常程序不容易被区别开来，在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在短时间内感染大量程序。而且受到感染后，计算机系统通常仍能正常运行，用户不会感到有任何异常。试想，如果病毒在传染到计算机上之后，机器会马上无法正常运行，那么它本身便无法继续进行传染了。

正是由于其隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散到其他计算机中。大部分病毒的代码之所以设计得非常短小，是为了隐藏。多数病毒一般只有几百或几千字节，而计算机对文件的存取速度比这要快得多。病毒将这短短的几百字节加入到正常程序之中，使人们不易察觉。

❑ **潜伏性**

大部分病毒在感染系统之后不会马上发作，它可以长时间隐藏在系统中，只有在满足其特定条件时表现（破坏）模块才会运行。只有这样才可以进行广泛的传播。如“PETER-2”在每年 2 月 27 日会提出 3 个问题，用户答错后将会把硬盘加密。著名的“黑色星期五”在每逢 13 号的星期五发作。国内的“上海一号”会在每年 3、6、9 月的 13 日发作。当然，最令人难忘的便是 4 月 26 日发作的 CIH 病毒。这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。

❑ **破坏性**

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响。良性病毒可能只显示些画面或发出点音乐、无聊的语句，或者根本没有任何破坏动作，只是会占用系统资源。但恶性病毒则有明确的目的，或破坏数据、删除文件或加密磁盘、格式化磁盘，有的甚至对

数据造成不可挽回的破坏。

❑ **不可预见性**

从对病毒的检测方面来看，病毒还有不可预见性。不同种类的病毒，它们的代码千差万别，但有些操作是共有的，如驻留内存等。有些人利用病毒的这种共性，制作了声称可以查找所有病毒的程序。这种程序的确可以查出一些新病毒，但由于目前的软件种类极其丰富，且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用这种方法对病毒进行检测势必会产生许多误报。而且病毒的制作技术也在不断地提高，病毒对反病毒软件永远是超前的。

2.2.3　网管心得——计算机病毒的防范措施

随着计算机及计算机网络的发展，计算机病毒传播问题越来越引起人们的关注。随着Internet的流行，计算机病毒又可以借助网络迅速传播，如“冲击波”病毒、灰鸽子等，给广大计算机用户带来了极大的损失，因此，为了避免或减小病毒所造成的损失，用户应该有正确的计算机病毒防范措施。

1．使用杀毒软件并安装系统安全漏洞补丁

用户应养成及时下载最新系统安全漏洞补丁的安全习惯，从根源上杜绝黑客利用系统漏洞攻击用户计算机的病毒。同时，升级杀毒软件、开启病毒实时监控应成为每日防范病毒的必修课。

2．重要资料必须备份

资料是最重要的，程序损坏了可重新下载安装，甚至再买一份，但是自己输入的资料，可能是三年的会计资料，可能是画了三个月的图片，结果某一天，硬盘坏了或者因为病毒的因素而丢失或破坏，会让人欲哭无泪，所以一般性的备份是绝对必要的。

3．网页挂马病毒的预防措施

网页挂马指的是黑客自己建立带毒网站，或者攻击流量大的现有网站，在其中植入木马、病毒，用户浏览这样的网站后就会中毒。由于通过“网页挂马”可以快速地入侵大量计算机，窃取用户资料，因此“挂马”成为利欲熏心的入侵者的首选入侵手段，防范网页挂马包括如下3个方面内容。

❑ 利用Windows Update功能打全系统补丁，避免病毒以网页挂马的方式入侵到系统中。

❑ 将应用软件升级到最新版本，其中包括各种IM即时通信工具、下载工具、播放器软件、搜索工具条等；不要登录来历不明的网站，避免病毒利用其他应用软件漏洞进行木马病毒传播。

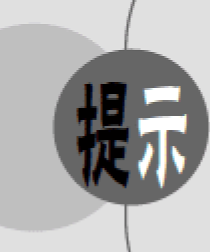
❑ 当有未知插件提示是否安装时，请首先确定其来源。

4．利用U盘进行传播的病毒的预防措施

据统计，2007年上半年，大约1/3的病毒可以通过U盘传播。在Windows系统下，当U

盘、MP3、移动硬盘等移动介质插入电脑时，系统会自动播放光盘上的电影、启动安装程序等，该功能给普通用户带来了很大方便，但这也成为用户计算机安全最为脆弱的地方，移动介质上的病毒会直接进入用户计算机，对于此有如下防范措施。

- 在使用移动介质（如U盘、移动硬盘等）之前，建议先对其进行病毒查杀。
- 尽量避免在无防毒软件的机器上，使用可移动磁盘。
- 禁用系统的自动播放功能，防止病毒从U盘、移动硬盘、MP3等移动存储设备进入到计算机。



通过执行【开始】|【运行】命令，在弹出的对话框中，输入gpedit.msc命令，按回车键，在打开的【本地组策略编辑器】窗口中，依次展开【计算机配置】|【管理模板】节点，选择【系统】选项，双击右侧窗格中的【关闭自动播放】选项，在弹出的对话框中，选中【已启用】单选按钮，并单击【确定】按钮，即可禁用Windows系统的自动播放功能。

- 尽量不要使用双击打开U盘，而是右击U盘图标，执行【打开】命令来打开。

5. 网上银行、在线交易的预防措施

随着电子商务的普及、股市的火爆，在线交易、网上炒股成为流行，有关网络银行和股票账号的病毒数量一直呈上升趋势。而且，2007年上半年入市的新股民中，很多属于中老年用户，他们对计算机和网络缺乏基本的安全概念，在遭受病毒侵害后将面临更大的安全损失。

通常，用户可以通过如下措施来预防在线交易、网上炒股时遭到病毒破坏。

- 在登录电子银行实施网上查询交易时，尽量选择安全性相对较高的USB证书认证方式。不要在公共场所（如网吧）登录网上银行等一些金融机构的网站，防止重要信息被盗。
- 网上购物时也要选择注册时间相对较长、信用度较高的店铺。
- 不要随便点击不安全陌生网站，如果遇到银行系统升级要求更改用户密码或输入用户密码等要求，一定要提前确认。如果用户不幸感染了病毒，除了用相应的措施查杀病毒外，也要及时和银行联系，冻结账户，并向公安机关报案，把损失减少到最低。
- 在登录一些金融机构，如银行、证券类的网站时，应直接输入其域名，不要通过其他网站提供的链接进入，因为这些链接可能将导入虚假的银行网站。

2.3 常见的计算机病毒类型

病毒的制造者不断地尝试新的方法来感染计算机系统。但是病毒的实际类型还是只有很少的几种。常见的计算机病毒包括文件型病毒、引导型病毒、宏病毒、电子邮件病毒和混合型病毒等。

2.3.1　文件型病毒

文件型病毒（File Infector Virus）通常寄生在可执行文件（如*.com、*.exe 等）中，当这些文件被执行时，病毒程序就会紧接着被执行。文件型病毒根据传染方式的不同，又包括非常驻型和常驻型两种。

❑ **非常驻型病毒**

非常驻型病毒（Non-memory Resident Virus）将自己寄生在*.com、*.exe 或者*.sys 文件中。当这些中毒的程序被执行时，就会尝试传染给另一个或多个文件。

❑ **常驻型病毒**

常驻型病毒（Memory Resident Virus）驻留在内存当中，其行为就好像是寄生在各类的低阶功能一般（如中断），由于这个原因，常驻型病毒往往对磁盘造成更大的伤害。一旦常驻型病毒进入了内存中，只要存在可执行文件被执行，它就会对其进行感染，其效果非常显著。将它赶出内存的唯一方式就是冷开机（完全关掉电源之后再开机）

病毒感染 COM 文件有两种方法，一种是将病毒加在文件前部，一种是将病毒加在文件尾部，如图 2-1 所示。

EXE 文件较为复杂，每个 EXE 文件都有一个文件头，当 DOS 加载 EXE 文件时，根据文件头信息，病毒一般会将自己加在文件尾部，并修改文件头信息，使开始执行地址指向病毒起始地址，并修改文件长度信息。

而 Windows 系统下的 EXE 文件与 DOS 下的有所不同，它除了具有 MS-DOS 的 EXE 文件头之外还包括一个 Windows 的 EXE 文件头，但它们的原理是一样的。

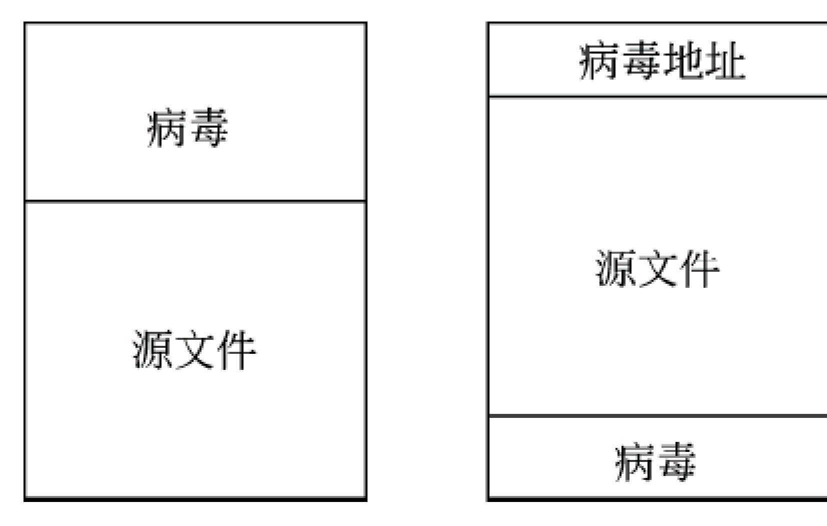


图 2-1　可执行文件病毒

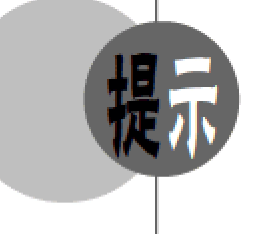
2.3.2　引导型病毒

引导型病毒利用引导扇区藏身，利用 IOS 中断执行破坏操作，利用 BIOS 数据区来使病毒代码常驻内存。

引导型病毒是在系统启动时，先于正常系统的引导将其自身装入到系统中，这是因为这类病毒侵占了系统磁盘的主引导区或者 DOS 分区的引导扇区，而系统在启动时只是机械地将这些扇区中的内容读入到内存中，这样病毒就可以获得对系统的控制权。病毒程序一般安装在内存的高端，为了保护病毒程序使用的这一部分内存区域不再被系统分配，一般病毒会将系统内存总量减少若干 K 字节。而正常的系统引导过程一般是不减少系统内存。

病毒程序在完成自身的安装后，再将系统的控制权交给真正的系统程序，完成系统的引导，但此时系统已经处于病毒程序的控制之下。

引导型病毒在进行自身的安装时，为了实现向外传播和破坏的作用，一般都要修改系统的某些中断向量，主要是 INT13H 中断向量，使之指向病毒程序的相应部分，在系统运行时，只要使用到这些中断向量，或者满足病毒程序设定的某些特定条件，病毒程序就会向外传播，或者对系统或数据进行破坏。



中断是指系统、处理器或当前执行程序（或任务）的某处出现一个事件，该事件需要处理器进行处理。通常，这种事件会导致执行控制被强迫从当前运行程序转移到称为中断处理程序的特殊软件函数或任务中。为了有助于处理中断，每个需要被处理器进行特殊处理的处理器定义的中断条件都被赋予了一个标识号，称为向量（Vector）。处理器把赋予中断的向量用作中断描述符表 IDT（Interrupt Descriptor Table）中的一个索引号，来定位一个中断的处理程序入口点位置。

系统引导型病毒的传染对象主要是硬盘的主引导扇区及硬盘的 DOS 分区的引导扇区。这类病毒是由含有病毒的系统感染在该系统中进行读写操作的移动磁盘，然后，再由这些移动磁盘以复制的方式（被动传染）和引导进入到其他计算机系统的方式（动态传染）去感染其他计算机的硬盘和计算机系统。如此循环下去，就使该病毒迅速传播。

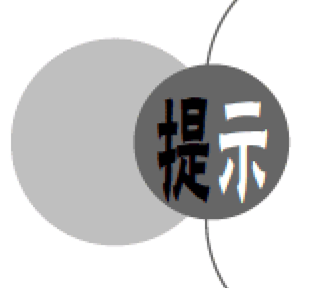
引导型病毒只能感染可执行代码，在计算机中，可执行代码只有引导程序和可执行文件，如果要了解引导型病毒的原理，首先就需要了解引导区的结构。通常，移动磁盘（如优盘）只有一个引导区，称为“DOS BOOT SECTER”，只要格式化优盘，该引导区就已存在。硬盘包括两个引导区，在 0 面 0 道 1 扇区的称为主引导区，内有主引导程序和分区表，主引导程序查找激活分区，该分区的第一个扇区即为 DOS BOOT SECTER。绝大多数病毒都是感染硬盘的主引导分区。

引导型病毒按其寄生对象的不同又可分为两类，即覆盖型（嵌入型）病毒和转移型（保留型）病毒。

❑ **覆盖型**

该类型病毒在传染磁盘引导区时直接用自身代码覆盖原引导记录，但并不触动分区表及检验标志 55AA（十六进制，主引导扇区的最后两个字节），且不保留备份，启动时由自身代码完成对系统的引导。

用户可以通过使用 NU DiskEdit 等工具来查看主引导记录映像表，在 IBE、ICE、IDE 和 IEE 四处，如果发现其中一项为 80，其他项为 00，那么可以认为存在覆盖型病毒；在 000、001、002 处为 FA 33 C0，在 080、081 处或 IFE、IFF 处是 55 AA，在 082～0DE 之间是规则的英文信息，在 170～1BD 之间全是 0，如果在这 5 处中有 3 处符合，则认为是覆盖型病毒。



主引导记录包括代码（如 IBE、ICE 等）、数据（如 00、80 等）两部分，用于检测硬盘分区的正确性并确定活动分区，负责把引导权移交给操作系统，如果此段记录损坏将无法从硬盘引导。所以硬盘的主引导区常常成为病毒攻击的对象。

❑ **转移型**

该类型病毒在传染磁盘引导区之前保留了原引导记录，并转移到磁盘其他扇区，以备将来病毒初始化模块完成后仍由原引导记录完成对系统的正常引导。如果根据覆盖型病毒的判定方法中的内容不能判定为覆盖型病毒，那么可认为该病毒是转移型病毒。

引导型病毒隐蔽性强，兼容性强，不容易被用户发现，通常用于 DOS、Windows 操作系统，图 2-2 为转移型病毒原理示意图。

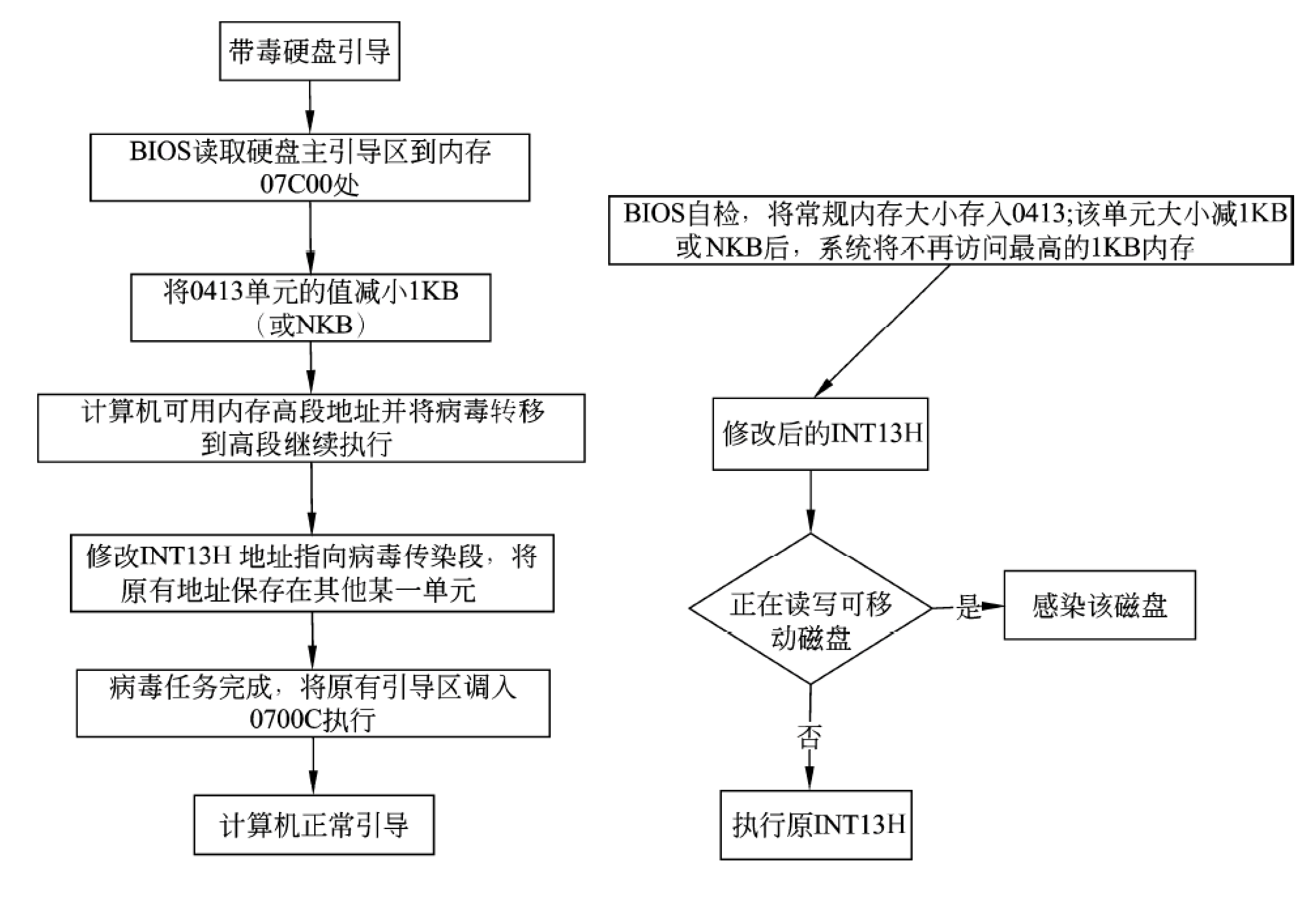


图 2-2　转移型病毒原理示意图

如果用带毒的可移动磁盘启动计算机，那么病毒首先感染硬盘，然后执行上述启动过程。无论是最古老还是最新的转移型病毒都遵循上述原理，只不过在实现时，技巧可能不相同。

2.3.3　宏病毒

宏就是软件设计者为了在使用软件工作时，避免一再地重复相同的动作而设计出来的一种工具。它利用简单的语法，把常用的操作写成宏，当再工作时，就可以直接利用事先写好的宏自动运行，去完成某项特定的任务，而不必重复相同的操作。

在 Word 中对宏定义为：宏就是能组织到一起作为独立的命令使用的一系列 Word 命令，它能使日常工作变得更容易。Word 宏是使用 Word Basic 语言来编写的。

每个 Word 宏都有其触发条件，可以将宏与工具条按钮、菜单项或者热键联系起来。但按住该按钮、选择该菜单项或者按住该热键时，这个宏就会被执行。

凡是具有写宏能力的软件都有宏病毒（Macro Virus）存在的可能，如 Word、Excel、AmiPro 等都存在宏病毒。例如，台湾一号（Taiwan NO.1）就是 Word 宏病毒。

如果编写一个宏并将其命名为 AutoNew。那么当用户每次打开一个新文件时该宏都将被调用。对于一个新建立的宏，在退出 Word 时都会询问是否保存的提示，如果选择是，那么该宏就会被保存在公用模板文件 Normal.dotm 中，以后用户每次打开 Word 时都可以调用这个宏。另外，Word 允许每个文档本身包含私用宏，这些宏只能够在该文档打开时使用，关闭后不能使用。

由于 Word 本身所附带的 Word Basic 富含丰富的函数，熟练地使用 Word 宏可以大大提高用户的工作效率，达到事半功倍的效果。但是，它也为病毒的产生提供了条件。

Word 宏病毒就是利用 Word 包含的宏功能作为撰写病毒的工具。公用模板文件 Normal.dotm 为宏病毒的侵入开启了一扇大门。当宏病毒感染公用模板文件后，一旦用户打开 Word，那么这个受感染的公用模块文件即被载入，病毒便会传播到随后所编辑的 doc 文件中。

被感染的 Word 文件中通常包含有 Auto Open、Auto Close 和 Auto New3 个宏。当用户使用正常的 Word 软件打开被感染的 doc 文件后，该文件中的 Auto Open 宏被自动执行，然后，通过 Auto Close 和 Auto new 这两个宏也将会被复制到公用模块文件 Normal.dotm 中，从而使正常的 Word 也感染病毒。

虽然不是所有包含宏的文档都包含宏病毒，但当有如下情形之一发生时，用户就可以检测出 Microsoft Office 文档或 Microsoft Office 系统中存在宏病毒。

❑ **在打开“宏病毒防护功能”的情况下**

当用户打开一个自己编写的文档时，系统会弹出相应的警告框。而用户清楚自己并没有在其中使用宏或并不知道宏到底怎么用，此时就可以判断出该文档已经感染宏病毒。

另外，用户在打开 Microsoft Office 系列文档时都看到宏警告信息。由于在一般情况下很少使用到宏，所以当看到成串的文档有宏警告时，可以判断出这些文档中有宏病毒。

❑ **如果软件中关于宏病毒防护选项启用后但不能在下次开机时保存**

在 Microsoft Office Word 97 中提供了对宏病毒的防护功能，它可以在【工具】|【选项】|【常规】中进行设定。但有些宏病毒为了对付宏警告功能，当它在感染系统（这通常只有在用户关闭了宏病毒防护选项或者出现宏警告后选取了“启用宏”才有可能）后，会在退出 Microsoft Office 文档时自动屏蔽掉宏病毒防护选项。因此用户一旦发现计算机中所设置的宏病毒防护功能选项无法在两次启动 Word 之间保持有效，那么说明计算机系统已经感染了宏病毒。也就是说一系列 Word 模板，特别是 Normal.dotm 已经被感染。

当用户发现计算机存在宏病毒后，根据宏病毒的传播原理，就可以很轻松地清除它。消除宏病毒只需用户在 Normal.dotm 和 doc 文件中删除构成病毒的宏即可。在 Word 文档中，执行【开发工具】|【宏】命令，在打开的【宏】对话框中的【宏的位置】下拉列表框中选择 Normal.dotm 选项或者其他有毒的 Word 文档，然后，再选择需要删除宏的名称，单击【删除】按钮即可，如图 2-3 所示。



图 2-3　清除宏病毒

2.3.4　蠕虫病毒

蠕虫（Worm）病毒是一种通过网络进行传播的恶意病毒，它的出现相对于木马病毒、宏病毒来说比较晚，但是无论从传播速度、传播范围还是从破坏程度上来讲，蠕虫病毒都是以往的传统病毒所无法比拟的。

蠕虫病毒可以说是近年来发作最为猖獗、影响最为广泛的一类计算机病毒，它的传播主要体现在以下两个方面。

❑ 系统漏洞

利用微软的系统漏洞攻击计算机网络，网络中的客户端感染这一类病毒后，会自动拨号上网，并利用文件中的地址或者网络共享传播，从而导致网络服务遭到拒绝并发生死锁，最终破坏用户的大部分重要数据。“红色代码”、“尼姆达”、“SQL 蠕虫王”等病毒都是属于这一类病毒。

❑ 电子邮件

利用 E-mail 迅速传播，如“爱虫病毒”和“求职者病毒”。蠕虫病毒会盗取被感染计算机中邮件的地址信息，并且利用这些邮件地址复制自身病毒体以达到大量传播、对计算机造成严重破坏的目的。蠕虫病毒甚至可以导致整个互联网的瘫痪。

1. 蠕虫病毒的构成

蠕虫（Worm）病毒通常由主程序和引导程序两部分组成。其中，主程序的主要功能是搜索和扫描，这个程序能够读取系统的公共配置文件，获得与本机联网的客户端信息，检测到网络中的哪台计算机没有被占用，从而通过系统的漏洞，将引导程序建立到远程计算机上；引导程序实际上是蠕虫病毒主程序（或一个程序段）自身的一个副本，而主程序和引导程序都有自动重新定位（Auto relocation）的能力。即这些程序或程序段都能够把自身的副本重新定位在另一台机器上，如图 2-4 所示。这就是蠕虫病毒能够大面积暴发并且带来严重后果的主要原因。

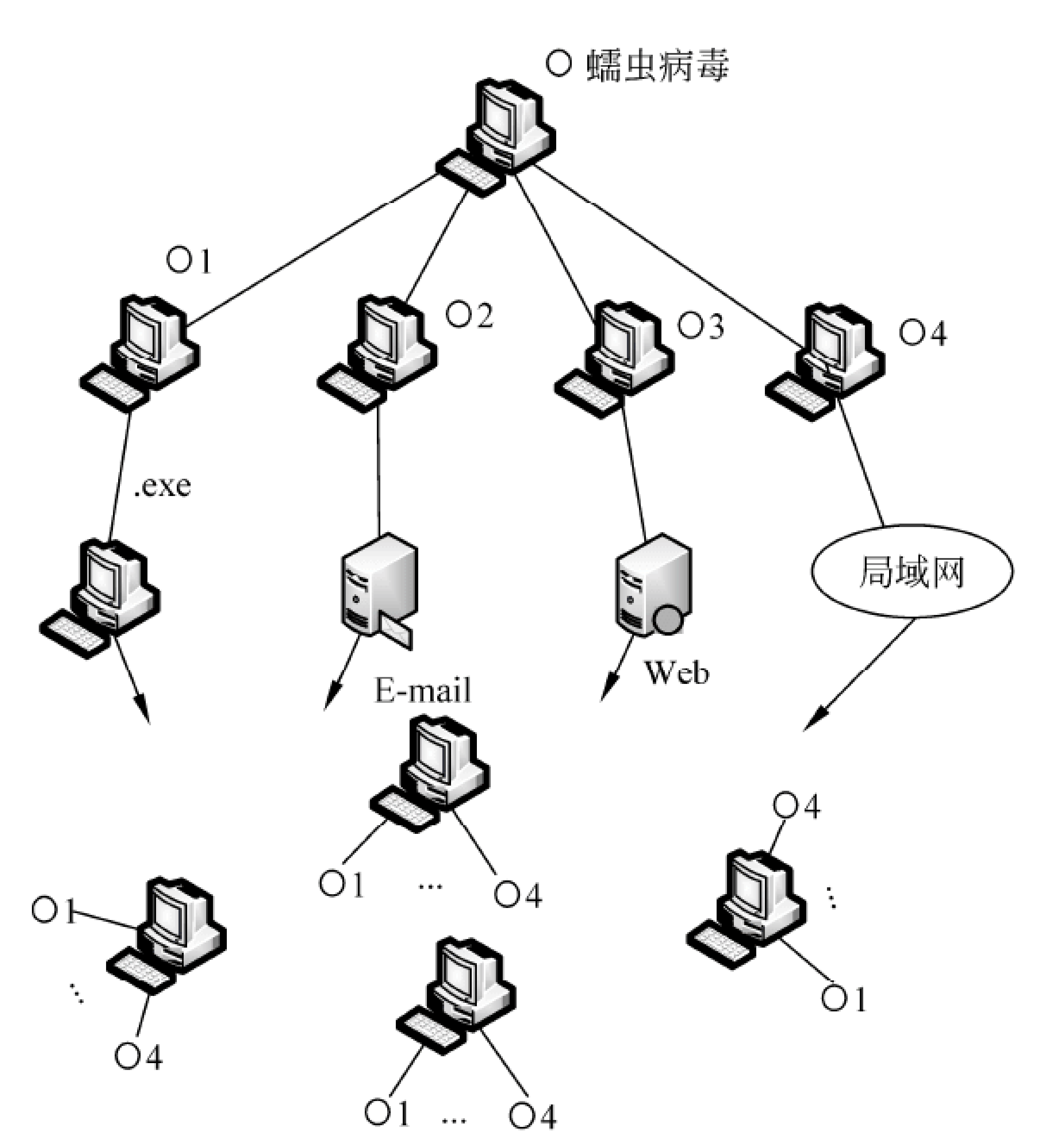


图 2-4　主程序和引导程序将其副本定位在另一台计算机上示意图

2. 蠕虫病毒的特点及发展趋势

❑ 利用操作系统和应用程序的漏洞主动进行攻击

此类病毒主要包括“红色代码”和“尼姆达”以及至今依然肆虐的“求职者”等。由于

IE 浏览器的漏洞，使得感染了“尼姆达”病毒的邮件在不通过手工打开附件的情况下就能激活病毒，而此前很多防病毒专家还一直认为：“只要不打开带有病毒的邮件的附件，病毒就不会造成危害”。“红色代码”是利用了微软 IIS 服务器软件的漏洞（idq.dll 远程缓存区溢出）来传播的。“Sql 蠕虫王”病毒则是利用了微软数据库系统的一个漏洞进行攻击的。

- ❑ **传播方式多样化**

例如，“尼姆达”病毒和“求职者”病毒可利用的传播途径包括文件、电子邮件、Web 服务器及网络共享等。

- ❑ **病毒制作技术与传统病毒不同**

许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改，从而可以产生新的变种，因此可以逃避反病毒软件的搜索。另外，新病毒利用 Java、ActiveX、VB Script 等技术，可以潜伏在 HTML 页面里，在用户浏览网页时被触发。

- ❑ **与黑客技术相结合**

与黑客技术相结合后潜在的威胁和损失更大。以“红色代码”为例，感染后的计算机在 Web 目录的\scripts 下将生成一个 root.exe 应用程序，通过该程序可以使黑客远程执行任何命令，达到再次进入的目的。

3. 蠕虫病毒发作现象及防范

蠕虫病毒进入系统并且成功运行后，会搜索当前系统中 Outlook 通信簿中存储的邮件地址，每当搜索到一个邮件地址时就会自动生成一个邮件，然后将病毒文件作为邮件的附件，并且将附件的名称更改为一个比较具有诱惑力的名字（如“你的银行密码”、“美女图片”等）以吸引邮件接收者打开附件。

一般病毒生成的邮件都会带有“自动启动漏洞”功能，即当用户打开邮件的时候其附件就会自动启动，这个过程非常快，一般不会被用户发现。这种具有漏洞的邮件用文本编辑器打开后会发现漏洞代码，如图 2-5 所示。带有这种代码的邮件一般都比较可疑。而且打开这种邮件后，根本看不到已经运行的病毒附件，只能看到一些病毒生成的用于迷惑人的信息。



```
X-OriginalArrivalTime: 16 Jul 2002 07:15:06.0620 (UTC) FILETIME=[831D93C0:01
Date: 16 Jul 2002 15:15:06 +0800

--11db82sd319dm2ns0f4383dhG
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable

<HTML><HEAD></HEAD><BODY>
<FONT COLOR=#FF0000>
<b>ATTENTION!</b><br><br>
You can access<br>
<b>very important</b><br>
information by<br>
this password<br><br>
<b>DO NOT SAVE</b><br>
password to disk<br>
use your mind<br><br>
now press<br>
<b>cancel</b><br><br>
(liuzhenhua)</font></BODY></HTML>
<iframe src=3Dcid:W8dqwq8q918213 height=3D0 width=3D0></iframe>

--11db82sd319dm2ns0f4383dhG
Content-Type: audio/x-midi;
        name=decrypt-password.exe
Content-Transfer-Encoding: base64
Content-ID: <W8dqwq8q918213>

TVqQAAMAAAAEAAAA//8AAIgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA8AAAAA4fug4AtAnNIbgBTMOhVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4g
RE9TIG1vZGUuDQ0KJAAAAAAAAAAvUy/dazJBjmsyQY5rMkGOMhFSjmkyQY4QLk2OYzJBjugu
T45/MkG0gylLjg4yQY6DLUq0YzJBjmsyQY5jMkGOCS1SjnAyQY5rMkCOATJBjoMtV451MkG0
```

图 2-5　漏洞代码

蠕虫病毒的出现可以说是网络管理员的一个噩梦。面对快速复制和疯狂传播的病毒，除了使用网络版杀毒软件进行全网监控和全网查杀之外，还有几点需要客户端使用者与管理员互相配合，共同防范。

- ❑ 购买主流的网络安全产品，并注意及时更新。
- ❑ 不随意查看陌生邮件，尤其是带有附件的邮件。
- ❑ 定期检查计算机内是否具有可写权限的共享文件夹，一旦发现，要及时关闭该权限。
- ❑ 定期检查计算机中的账户，查看是否存在不明账户。一旦发现应立即删除该账户，并

且要禁用 Guest 账号，以防止被病毒利用。

- 用户在网络中共享的文件夹一定要将访问权限设置为只读，而且最好给共享文件夹设置一个访问账号和密码。这样病毒在传播的过程中会因为权限不够而造成复制失败。
- 给计算机中的账户设置比较复杂的密码，以防止被病毒破译。如果在自己的共享文件夹内发现了不明文件，最好将其删除，千万不要尝试打开甚至启动运行。

网络工具列表（常见的杀毒软件）

1. 瑞星软件应用

北京瑞星科技股份有限公司，简称瑞星软件公司，成立于 1998 年 4 月，其前身为 1991 年成立的北京瑞星电脑科技开发部，是中国最早从事计算机病毒防治与研究的大型专业企业。它以研究、开发、生产及销售计算机反病毒产品、网络安全产品和反“黑客”防治产品为主，拥有全部自主知识产权和多项专利技术。

早期，瑞星软件公司产品为瑞星防病毒卡，这是一块 ISA 界面的硬件产品，通过截取 DOS 系统中断来保护计算机磁盘数据，这是一种在 1990 年代初期较为流行的防病毒手段，当时瑞星公司的产品占据了中国防病毒卡市场的一半以上。

随着计算机硬件技术、网络技术的不断发展，瑞星软件公司为满足广大用户的需求，所生产的产品应用于不同领域、不同用户。目前，瑞星杀毒软件系列包括网络版和单机版，提供杀毒软件、个人防火墙、在线杀毒等功能，且提供简体中文、繁体中文、英文、日文等多种语言版本。另外，瑞星软件公司同时还提供企业网络监控软件，并且与硬件厂商合作推出硬件病毒防火墙产品。因此，瑞星软件公司提供的软件应用十分广泛，适合大部分用户使用。

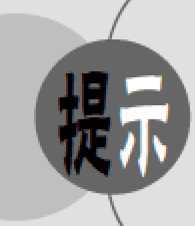
下面以瑞星个人防火墙为例来简单介绍。瑞星个人防火墙（Rising Personal Firewall）是一款防火墙软件。其主要应用就是能够针对目前流行的黑客攻击、钓鱼网站等做出针对性的优化，采用未知木马识别、家长保护、反网络钓鱼技术来保护用户的计算机系统不受侵害。

目前，最新的瑞星防火墙版本为 2010 版，用户可以下载或购买瑞星个人防火墙并安装，然后，启动并打开【瑞星个人防火墙】主界面，如图 2-6 所示。



图 2-6 【瑞星个人防火墙】主界面

在【瑞星个人防火墙】主界面左侧窗格中，用户可以根据实际网络环境来定义安全级别（如高、中和低）、工作模式（常规模式、交易模式和静默模式），在右侧窗格中，用户可以查看到当前上网流量图以及当前活动的程序。



软件默认工作在常规模式，如果用户需要进行网上交易，那么可以使用交易模式，以确保个人账户的安全。当用户选择静默模式时，软件会自动处理发现的病毒和恶意程序。

选择【系统信息】选项卡，用户可以查看到当前正在运行的程序，切换到【进程信息】选项卡下，用户可以很容易地查看到当前运行的进程是否安全，如图 2-7 所示。

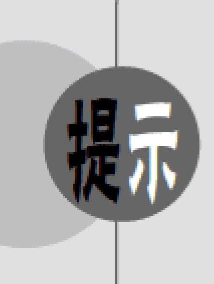


图 2-7　查看进程信息

选择【网络安全】选项卡，用户可以查看到防火墙对当前网络的监控列表，通常，未开启 ARP 欺骗防御，如果用户上网环境处于局域网当中，那么建议用户启用 APR 欺骗防御。如要启用 ARP 欺骗防御，只需用户选择【ARP 欺骗防御】选项，并单击【开启】按钮即可，如图 2-8 所示。



图 2-8　开启 ARP 欺骗防御



ARP 地址解析协议是一种常用的网络协议，每台安装有 TCP/IP 协议的计算机中都有一个 ARP 缓存表，表中的 IP 地址与 MAC 地址一一对应，如果这个表被修改，则会出现网络无法连通，或者访问的网页被劫持。黑客就会利用 ARP 协议存在的缺陷，入侵某台计算机之后发送 ARP 欺骗数据包，造成局域网内所有用户在访问网络时，都会收到这样的数据包。

另外，如果用户不希望某一程序访问网络还可以通过访问控制来实现。在【访问控制】选项卡中右击需要阻止的程序名称，并执行【拒绝】命令即可，如图 2-9 所示。



图 2-9　设置访问控制

2．诺顿软件应用

赛门铁克（Symantec）公司总部位于美国加州，成立于 1982 年 4 月，原为编程语言公司。但在 1990 年，该公司收购彼得 • 诺顿（Peter Norton Computing）软件公司，才正式跨入杀毒软件市场，而诺顿（Norton）是该公司推出的个人信息安全产品之一。

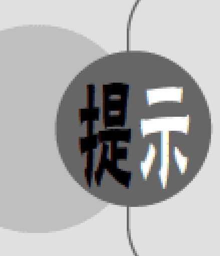
诺顿杀毒软件应用于广大用户、小型单位或公司以及大型企业，能够确保网络安全及解决安全问题，保护广大消费者的计算机免于病毒爆发或恶意程序攻击。

诺顿杀毒软件发展至今，除了原有的防毒功能外，还有防间谍等网络安全风险的功能。目前，诺顿反病毒产品包括诺顿网络安全特警（Norton Internet Security）、诺顿防病毒（Norton Antivirus）、诺顿 360 等产品。

目前，诺顿反病毒软件的最新版本包括诺顿网络安全特警 2010、诺顿防病毒软件 2010、诺顿 360 4.0 版本和诺顿 360 Network 版。它们都能应用于计算机或网络核心防护、高级防护和身份防护。

- **核心防护**　通过核心防护，可以有效阻止病毒、间谍软件、特洛伊木马、蠕虫病毒等的侵害。诺顿软件为给系统提供最新的防护会每隔 5~15 分钟执行一次更新。
- **高级防护**　使用专业级反垃圾邮件技术过滤不受欢迎的电子邮件，防止利用软件漏洞

发起的网络工具及阻止传统防病毒软件不能识别的威胁。另外，它还提供家长控制功能，能够确保孩子上网安全（仅适用于 Microsoft Windows）。



与其他软件相比，诺顿防病毒软件功能较少，如该软件的高级防护功能，仅包括能够防止利用软件漏洞发起的网络攻击和阻止传统防病毒技术所不能识别的威胁。

- **身份防护** 通过身份防护能够存储和管理个人登录信息的安全，识别不安全的网站，防止黑客窃取用户个人信息。

除此之外，诺顿软件还具有许多实际应用，例如，诺顿网络安全特警 2010 和诺顿防病毒软件 2010 还提供计算机优化功能（如通过磁盘清理以优化计算机性能、对计算机近期整体行为做出明确分析以防止性能下降等）；诺顿 360 4.0 版本能够将用户重要文件自动保存在本地或保存至安全的其他存储位置以及能够还原丢失的文件和文件夹。

3. 卡巴斯基

卡巴斯基实验室总部位于莫斯科，主要为个人用户、企业网络提供反病毒、防黑客和反垃圾邮件产品，现已成为市场领先的信息安全解决方案提供商。

卡巴斯基实验室是第一个开发出诸多反病毒行业技术标准的公司，这些标准包括针对 Linux、UNIX 和 NetWare 的全面解决方案、能够用于检测新出现病毒的新一代启发式分析程序、防止多态性病毒和宏病毒的有效保护技术、持续更新反病毒数据库技术，以及检测档案文件病毒技术。

目前，卡巴斯基反病毒安全软件 2010 和卡巴斯基全功能安全软件 2010 都是该公司的新产品。其中，卡巴斯基全功能安全软件 2010 包含卡巴斯基反病毒软件 2010 的所有功能和技术。在该产品中集合了基于主机的入侵防御系统（HIPS）技术以及先进的应用程序活动控制技术，可以对新出现或者未知的程序划分安全等级，能够为个人计算机用户提供抵御各类互联网威胁的全面保护。

另外，该产品首次运用安全免疫区技术，利用虚拟化技术提供一个安全、独立的应用程序执行环境，当该软件安装完成后，在【我的电脑】窗口中将会查看到该文件夹，如图 2-10 所示。



图 2-10 【我的电脑】窗口

卡巴斯基全功能安全软件 2010 还为用户提供了卡巴斯基安全网络，一种创新的分布式恶意软件控制系统。该软件可以让用户拥有一段时间的试用期，用户可以从其官网进行下载或者试用结束后再购买该软件进行安装，安装完成后启动并进入该软件主界面，根据提示更新病毒库即可，图 2-11 为该软件主界面，默认显示【保护中心】页面，在该页面中用户可以查看到文件和数据、系统及网络在线是否安全。同样在安全中心

中用户也可以查看到计算机的安全信息。



图 2-11　【卡巴斯基全功能安全软件 2010】主界面

除了病毒防护之外，该软件还为用户提供了一些实用工具以帮助用户更好地使用计算机。如要使用这项功能，只需选择【工具中心】选项卡，在【工具中心】页面可以看到它所提供的全部安全工具，如图 2-12 所示。



图 2-12　工具中心

用户可以根据自己的选择使用工具中心中所提供的工具，也可以定期使用其中的一些工具来提高计算机性能。例如，选择【其他工具】列表内的【活动痕迹清理】选项，在弹出的对话框中直接单击【下一步】按钮软件会自动搜索用户痕迹，当搜索完成后，在【搜索活动

痕迹已完成】窗口中，可以查看到当前软件所检测到的用户活动痕迹，此时，单击【下一步】按钮即可，如图 2-13 所示。

最后，在【清除用户活动痕迹完成】窗口中，根据需要还可以启用【每次退出卡巴斯基全功能安全软件时都清除活动痕迹】复选框，并单击【完成】按钮，如图 2-14 所示。

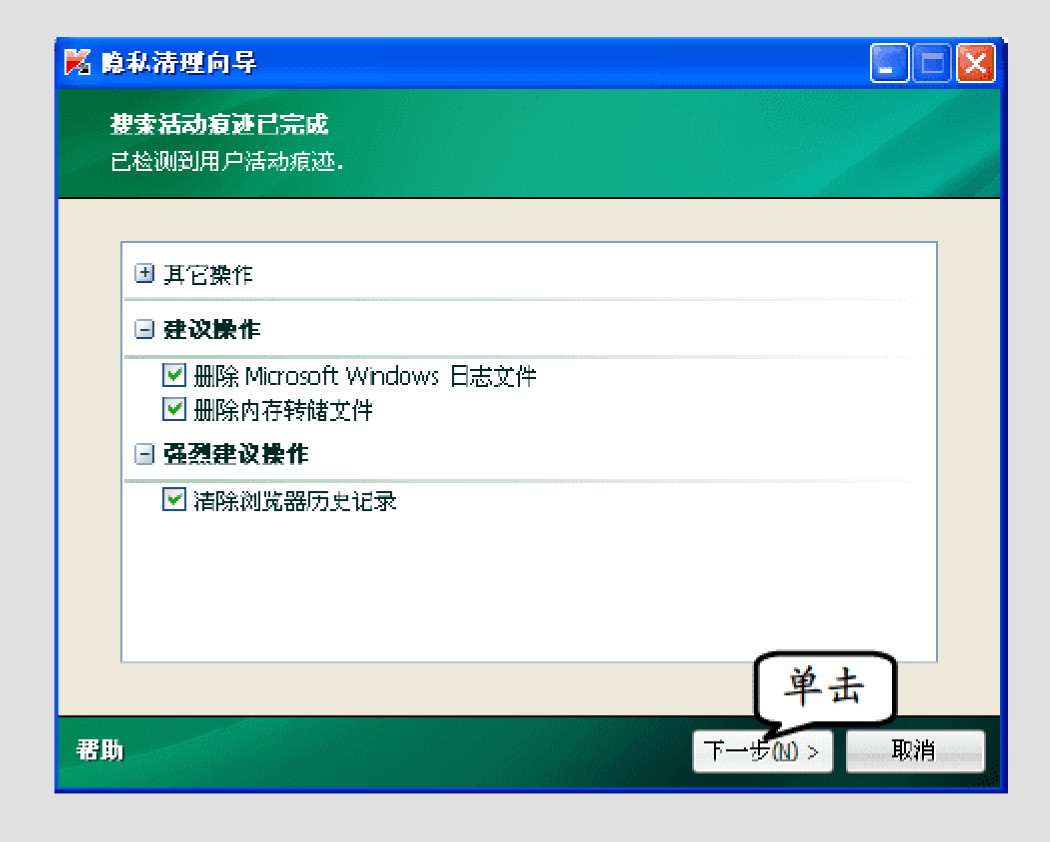



图 2-13　活动痕迹清理

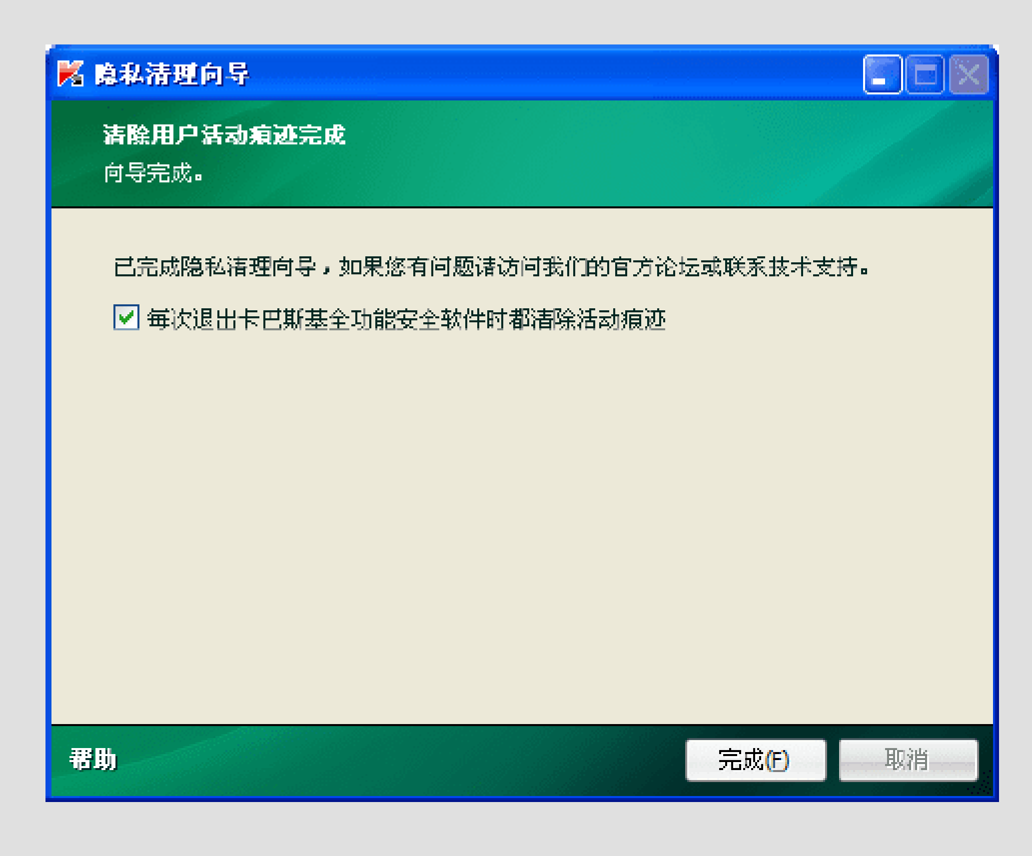


图 2-14　清理痕迹完成

另外，卡巴斯基实验室为每一位用户提供有效对抗病毒、垃圾邮件以及黑客攻击的安全解决方案。随着恶意软件程序变得日益复杂，功能也日趋增多，公司提供全方位的系列产品，以保护个人计算机用户和企业网络免受这些问题的困扰。例如，卡巴斯基反垃圾邮件旨在保护使用公司邮件系统的用户和互联网提供商免受垃圾邮件的困扰。

2.4　操作实例

2.4.1　操作实例——网页病毒的防范

用户在上网浏览网页的过程中，病毒可能已经进驻到计算机中，它们会使 IE 不停地弹出窗口、修改 IE 主页，甚至对系统性能造成非常大的影响，而通过使用一些软件可以很好地预防这些网页病毒，给用户一个舒适的上网环境。下面以超级兔子为例进行介绍。

1．实例目的

- 修复 IE 浏览器。
- 实现广告拦截。
- 保证浏览网页安全。

2．实例步骤

（1）在桌面双击【超级兔子】应用程序图标，如图 2-15 所示。

（2）在该软件主窗口中，单击【兔子工具】按钮，如图 2-16 所示。



图 2-15 执行应用程序



图 2-16 系统管理界面

（3）在【兔子工具】界面中，单击【守护天使】图标，如图 2-17 所示。

（4）在【守护天使】对话框的【选择修复项目】选项卡中，启用【IE 浏览器的标题与首页】复选框，然后单击【修复】按钮，如图 2-18 所示。



图 2-17 兔子工具界面

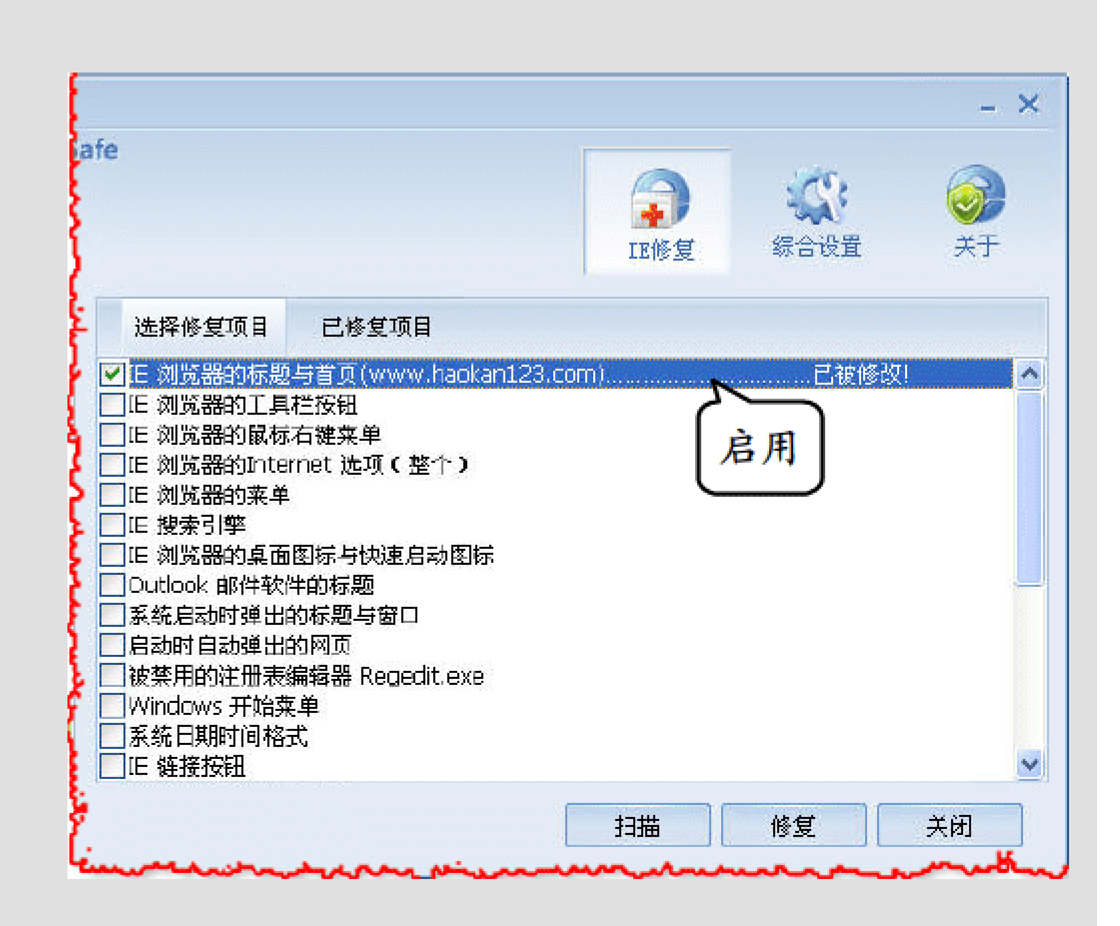


图 2-18 IE 浏览器修复界面

（5）在【已修复项目】选项卡中可查看到详细信息，然后单击【综合设置】按钮，如图 2-19 所示。



图 2-19 已修复项目界面



IE 修复是指为恢复被篡改的已设定的电脑浏览器主页而通过某一款软件进行的操作。

（6）在【综合设置】界面的【广告拦截设置】栏中，启用【拦截浮动广告】、【拦截弹出窗口】复选框，如图 2-20 所示。

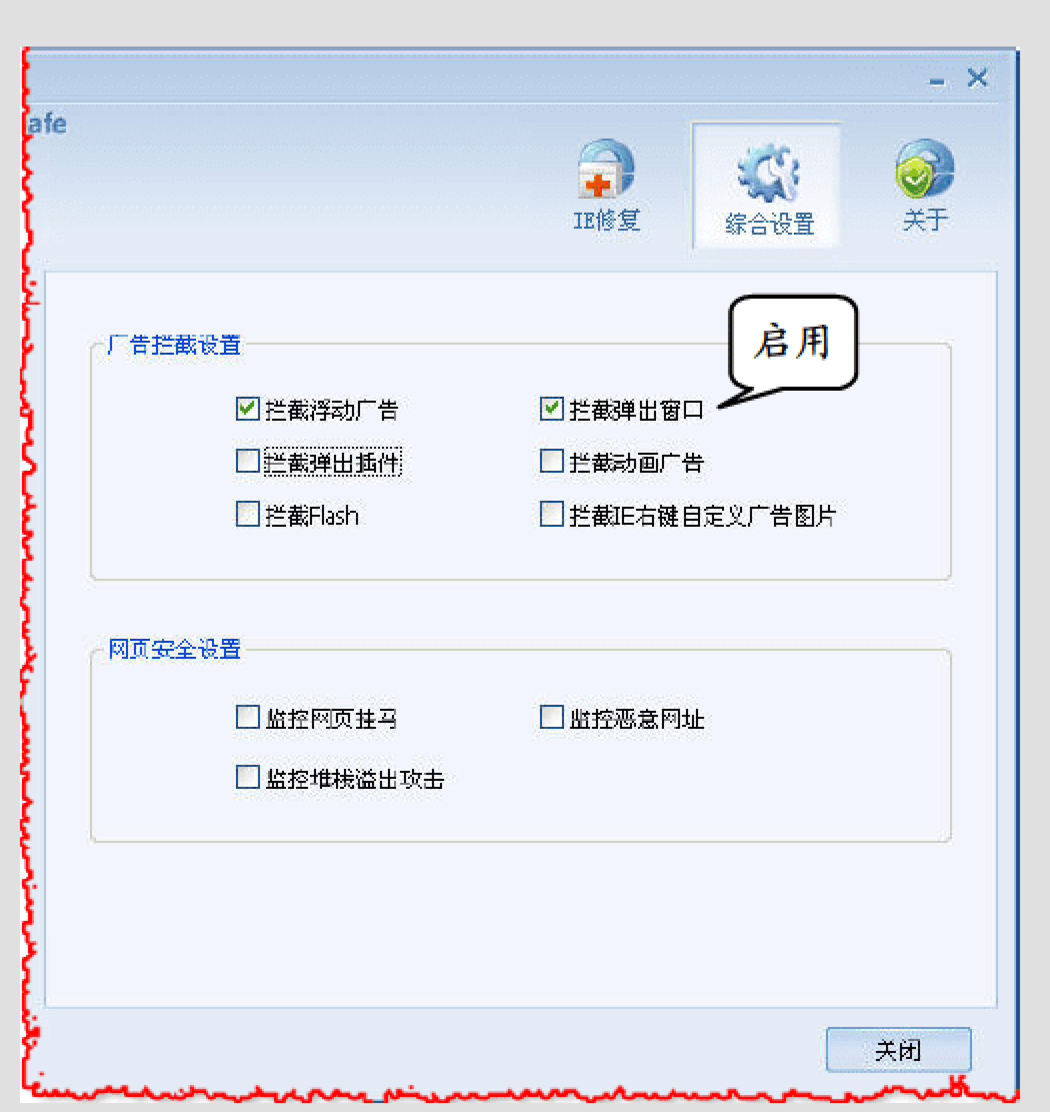


图 2-20　综合设置界面



广告拦截设置能成功拦截各种弹出广告，浮动图片，以及各种 Flash 插件，保证用户顺畅地浏览网页。

2.4.2　操作实例——手动清除 ARP 病毒

ARP 木马又称地址欺骗病毒，它使终端发送或接收虚假的 MAC 地址与 IP 地址对应关系来取代正确的对应关系，造成局域网不能正常通信。下面介绍清除它的方法。

1. 实例目的

- 清除 ARP 缓存。
- 设置 IP 地址与 MAC 地址绑定。
- 查找注册表。

2. 实例步骤

（1）执行【开始】|【运行】命令，在弹出的【运行】对话框中，输入 cmd 命令，并单击

【确定】按钮，如图 2-21 所示。

（2）在弹出的命令提示符窗口中，输入 arp –a 命令，可查看当前本机存储在本地系统 ARP 缓存表中的 IP 和 MAC 地址的对应关系信息，如图 2-22 所示。

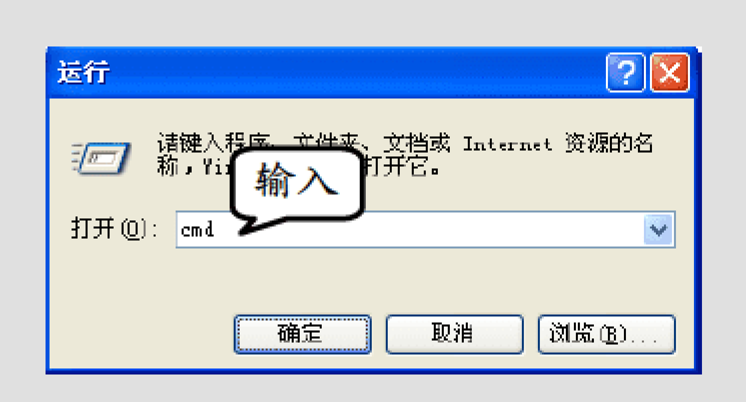


图 2-21　【运行】对话框

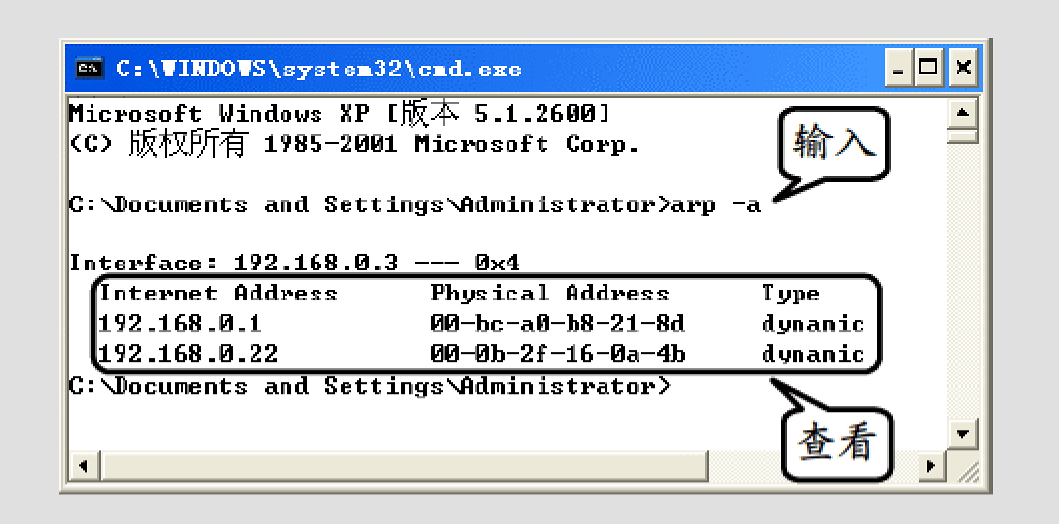
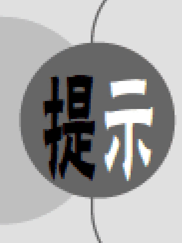


图 2-22　查看 ARP 缓存表

（3）在命令提示符窗口中，输入 arp –d 命令后，再次输入 arp –a 命令，可查看到 ARP 缓存表将被清空，如图 2-23 所示。



清除 ARP 缓存表可以解决某些因 ARP 欺骗工具攻击而导致局域网内计算机不能互相访问和上网的问题，清除之后，本机将重新从网络中获得正确的 ARP 信息，达到计算机之间互相访问与上网的目的。

（4）在命令提示符窗口中，输入 arp -s 192.168.0.3 00-E0-4C-A9-12-18 命令，并按回车键。然后，再输入 arp –a 命令，可查看 ARP 缓存表地址对应关系，如图 2-24 所示。

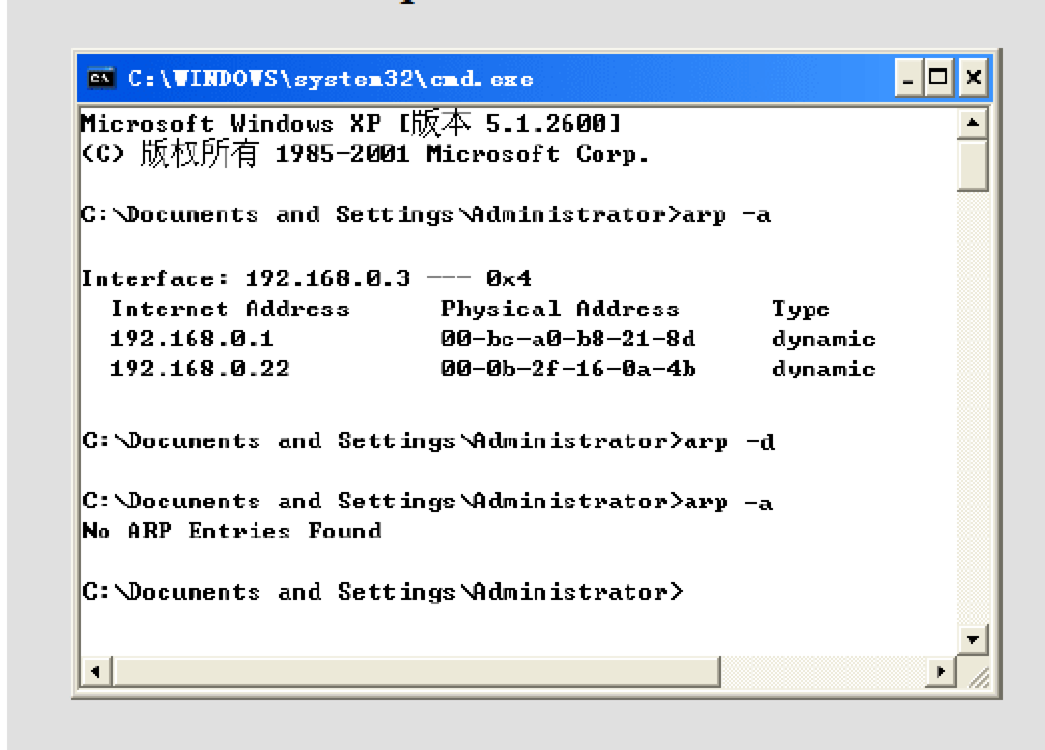


图 2-23　清除 ARP 缓存表

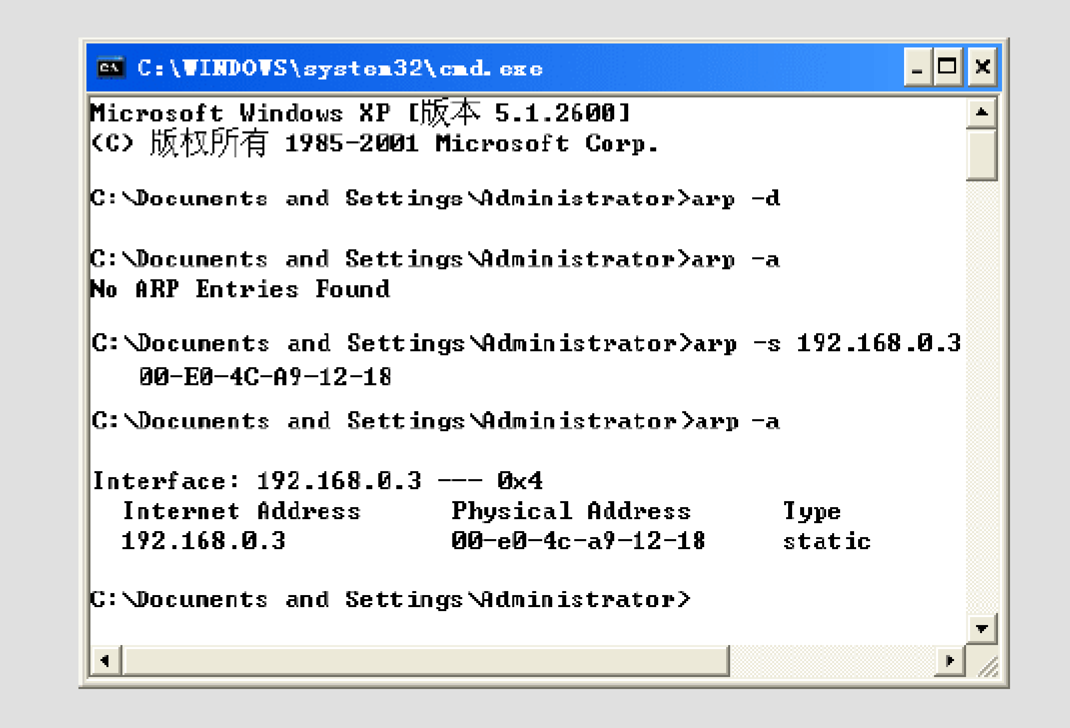


图 2-24　IP 地址与 MAC 地址绑定



将 MAC 地址与 IP 地址绑定，可以解决局域网内 ARP 病毒的攻击，但在计算机重新启动时，系统将自动清除 ARP 缓存信息，为此需要重新添加。

（5）执行【开始】|【记事本】命令，在弹出的记事本窗口中，输入批处理命令，并保存文件名为“mac ip.bat”，如图 2-25 所示。

（6）执行【开始】|【程序】|【启动】命令，在弹出的【启动】窗口中，将 mac ip.bat 文件复制到该路径下，如图 2-26 所示。

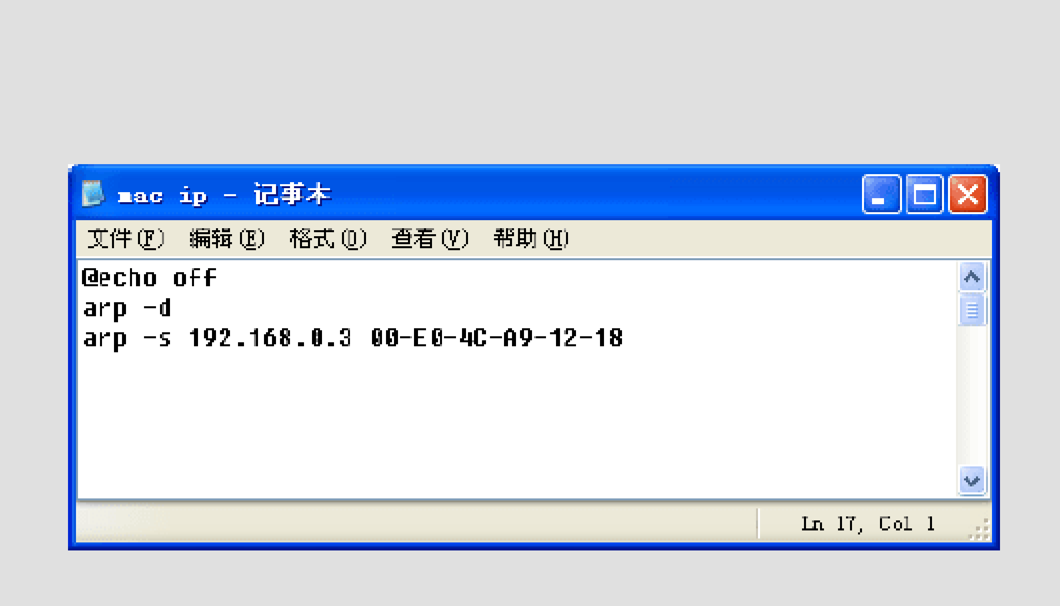
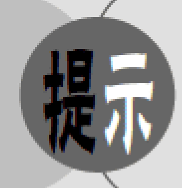



图 2-25　编写批处理内容



图 2-26　添加开机启动程序



mac ip.bat 批处理文件，可以解决计算机每次启动都要绑定 IP 地址与 MAC 地址的重复操作。

（7）执行【开始】|【运行】命令，在弹出的对话框中，输入 regedit 命令，并单击【确定】按钮，如图 2-27 所示。

（8）在弹出的【注册表编辑器】窗口中，执行【编辑】|【查找】命令，如图 2-28 所示。

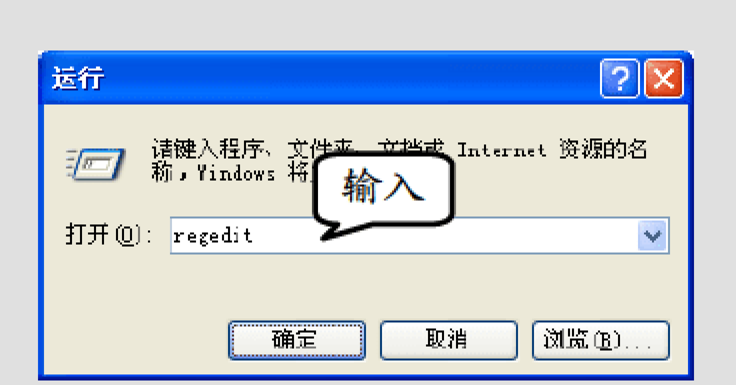


图 2-27　打开注册表

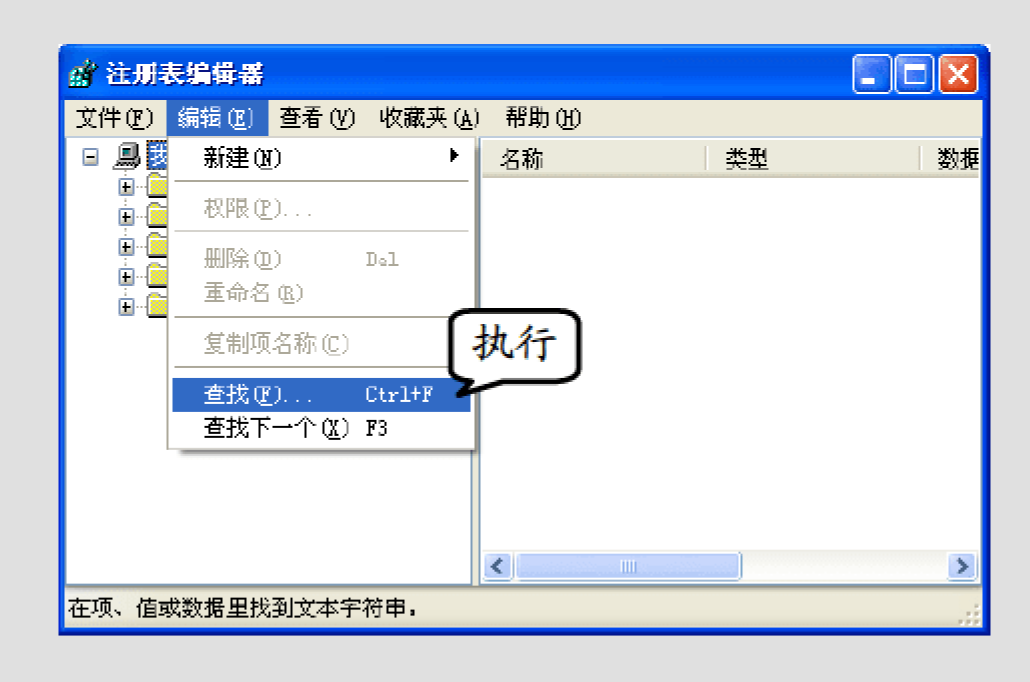


图 2-28　开始查找

（9）在弹出的【查找】对话框中，输入 npf.sys，如图 2-29 所示。然后，删除带有 npf 的文件即可。

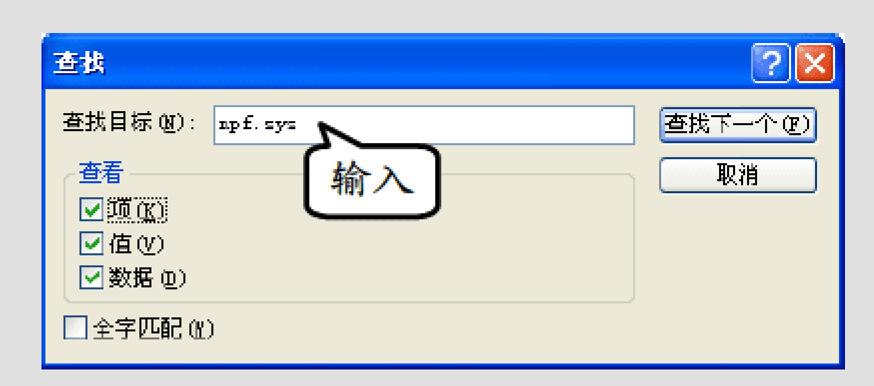


图 2-29　查找 npf 文件

（10）最后，为了以防万一，再使用杀毒软件检测一遍。

第3章 网络攻击与防范

计算机系统或信息会由于多种方式而发生不利的事情。这些不利的事情通常是人们有意（恶意的）进行的，也有是偶然导致的。但无论是什么原因，最后都会造成一定的损失，因此无论这些事情是否出于恶意都称为“攻击”。

黑客是指那些试图入侵计算机系统或使这些系统不可用的人。黑客及其工作方式是关于安全性的最重要的部分。因此，对网络与计算机安全的研究不能仅局限于防范，还要从非法获取目标计算机的系统信息、非法挖掘系统弱点等技术进行研究。对症下药，只有充分了解攻击者（黑客）的手段，才能够更好地采取措施来保护网络和计算机系统的正常运行。

本章从黑客的认识、常见的网络攻击及木马的攻击防护技术等方面来学习网络攻击与防范。

本章学习要点：

- 了解黑客的由来及黑客的行为发展趋势
- 熟悉攻击的分类及黑客的攻击目的
- 熟悉留后门与清痕迹的防范方法
- 熟悉木马的攻击与防护技术

3.1 黑客概述

在许多人眼中，“黑客”是这样一些高深莫测的神秘人物，他们利用手中所掌握的技术肆意攻击网络、盗取商业机密。加上一些媒体对黑客和黑客事件不负责任地夸大报道，使得黑客以及黑客技术对大多数普通人而言更多了一层神秘面纱。其实，黑客以及黑客技术并不神秘，也不高深。一个普通的用户在具备了一定的基础知识之后，就可以成为一名黑客，甚至在学会使用一些黑客软件后，同样有能力对网络实施攻击。

3.1.1 黑客的由来

黑客是“Hacker”的音译，源于英文动词 Hack，其引申意义是指“干了一件非常漂亮的事情”。

在牛津字典中，“Hacker”这个词是用来形容那些热衷解决问题、克服限制的人，并不单单指（限制于）电子、计算机或网络“Hacker”，“Hacker”的通性不是处于某个环境中的人所特有的，它的本质可以发挥在其他任何领域，如艺术等方面，事实上，在任何一种科学或艺

术的最高境界，都可以看到“Hacker”的特质。

黑客最早始于 20 世纪 50 年代，它们一般都是一些高级的技术人员，热衷于挑战、崇尚自由并且主张信息的共享。

1994 年以来，因特网在全球的迅速发展为人们带来了方便、自由和无限的访问，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来且随着计算机和网络技术的发展，黑客也随之出现。

黑客不干涉政治，不受政治利用，他们的出现推动了计算机和网络的发展与完善。黑客所做的不是恶意破坏，他们追求共享、免费，提倡自由、平等。黑客的存在是由于计算机技术的不健全，从某种意义上讲，计算机的安全需要更多的黑客去维护。

3.1.2 黑客的行为发展趋势

在早期，黑客是指专门研究、发现计算机和网络漏洞的计算机爱好者，他们伴随着计算机和网络的发展而不断成长。

黑客通常非常精通计算机硬件和软件知识，并有能力通过创新的方法剖析系统。他们通常会去寻找网络中存在的漏洞，但是往往并不去破坏计算机系统。黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找出漏洞，提出解决和修补漏洞的方法，从而帮助管理员进一步完善系统。

早期黑客的行为具有一定的职业道德，他们通常都遵循如下 12 条黑客守则。

- ❑ 不要恶意破坏任何系统，这样做只会给自己带来麻烦。
- ❑ 不要破坏别人的软件和资料。恶意破坏他人的软件将导致法律责任，如果只是使用计算机，那仅为非法使用，注意千万不要破坏别人的文件或数据。
- ❑ 不修改任何系统文件，如果是因为进入系统的需要而修改了系统文件，那么请在目的达到后将它改回原状。
- ❑ 不要轻易将要黑的或者黑过的站点告诉不信任的朋友。
- ❑ 在发表黑客文章时，不要使用真实姓名。
- ❑ 正在入侵时，不要随意离开自己的计算机。
- ❑ 不要入侵或破坏政府机关的主机。
- ❑ 将笔记放在安全的地方。
- ❑ 已入侵的计算机中的账号不得清除或修改。
- ❑ 可以为隐藏自己的入侵而作一些修改，但要尽量保持原系统的安全性，不能因为得到系统的控制权限而将门户大开。
- ❑ 不要做一些无聊的、单调且愚蠢的重复性工作。
- ❑ 做真正的黑客，读遍所有有关系统安全或系统漏洞的书籍。

但是，随着黑客的发展，有些黑客逾越尺度，运用自己的知识做出有损他人权益的事情，这些黑客逐渐被人们称为骇客（Cracker）。骇客指的是那些利用漏洞破坏网络安全的人，他们会通过计算机系统漏洞来入侵，他们也具备广泛的计算机知识，但与黑客不同的是，他们以破坏为目的。

遗憾的是，目前人们已经把黑客（Hacker）和骇客（Cracker）混为一谈，人们通常将入侵计算机系统的人称为黑客。

黑客在网上的攻击活动每年以 10 倍的速度增长，他们修改网页进行恶作剧，窃取网上信息兴风作浪，非法进入主机破坏程序、阻塞用户、窃取密码，进入银行网络转移金钱，进行电子邮件骚扰，黑客的破坏行为无孔不入。美国每年因黑客而损失近百亿美元。

从 20 世纪 50 年代，第一位黑客在麻省理工学院电子实验室诞生起，几十年来，有关黑客的重要事件如下所示。

- 1979 年，15 岁的凯文 · 米特尼克成功地入侵北美防空指挥部主机。
- 1983 年，由 6 位黑客组成的小组入侵了洛斯阿拉莫斯国家实验室。他们中年龄最大的仅 19 岁。
- 1987 年，赫尔伯特入侵美国电话公司，他也是黑客中第一位被判刑的人，当时年仅 17 岁。
- 1988 年，莫里斯导致了“蠕虫”事件。美国国防部不得不切断军事网与 ARPAnet 之间的物理连接。
- 1995 年，俄罗斯黑客列文盗取银行资金 370 多万美金，被判刑；同年，著名黑客凯文 · 米特尼克被捕。
- 1998 年，中国镇江黑客赫景华兄弟两人因盗窃银行资金被判死刑。
- 1999 年，网络迅速发展，同时一群技术刚刚起步的黑客开始建设自己的黑客网站。
- 从 1999 年到 2000 年间，中国黑客联盟、中国鹰派、中国红客联盟等一大批黑客网站兴起。
- 2000 年，雅虎、CNN 等各大网站遭到了 DDoS 的攻击，网络大面积瘫痪。
- 2001 年，8 月红色代码事件；9 月尼姆达事件；12 月 5 日，美国计算机安全事故协调中心（CERT）遭黑客攻击，造成该中心网站不能正常工作，该中心主任理查德·玻西亚说：“黑客攻击提醒我们，没有任何计算机系统是完全免疫的。”
- 2001 年 4 月 4 日，美国一些黑客组织相继对中国的一些政府、企业、教育、科研、电信等网站进行攻击。特别是中美撞机事件发生后，我国的一些黑客组织发起了一场网络反击战。这样便引发了一个具有历史意义的事件——中美黑客大战。
- 2003 年 1 月 SQL SLAMMER 事件。3 月口令蠕虫事件、红色代码 F 变种事件。8 月“冲击波”蠕虫事件。8 月 11 日，“冲击波”病毒开始在美国出现，随后不到一周之内，全球近 40 万台使用 Windows 系列操作系统的计算机均被感染。“冲击波”恶性计算机蠕虫病毒在全球范围内迅速泛滥，所到之处，计算机反复重新启动，文件大量丢失。美国联邦调查局经过调查宣称，他们找到了影响全球计算机的“冲击波”病毒制作者之一：一个年仅 18 岁的青年。9 月 9 日，以技术高超、神出鬼没而出名的美国黑客阿德里安 · 拉莫来到加利福尼亚的一家联邦法院自首，承认他在过去几年内曾成功入侵了 Google、雅虎、《纽约时报》等多家大型网站。
- 2004 年，美国当地时间 6 月 15 日早上，美国互联网服务公司 AKAMAI 受到黑客袭击，致使在两个小时的时间内，雅虎、Google 和微软等著名企业的网站无法正常登录。2004 年病毒和黑客的破坏行为仍然呈上升趋势，制造病毒越来越容易，病毒变种越来越多，出现得也越来越快，病毒和黑客越来越贪婪，骗术也越来越高明。

在我国，早在 1993 年，中科院高能所通过专线接入 Internet 时，国外黑客就入侵过高能所的系统。1996 年 2 月，刚开通不久的 Chinanet 受到攻击，并且得逞，不但网络上的主机系统遭受攻击，就是拨号上网的个人用户也受到牵连。2005 年 1 月，辽宁铁通的网络也遭受到黑客攻击，导致大量带宽用户不能上网。我国的黑客大致经历了以下几个阶段。

- **第 1 代（1996 年～1998 年）**

1996 年 Internet 在中国兴起，但是由于受到各种条件的限制，很多人根本没有机会接触网络。当时计算机在我国还没有达到普及的程度，大部分地区也没有开通因特网的接入服务，因此第 1 代黑客大多是从事科研工作的人，只有他们才有机会频繁地接触计算机和网络。

1998 年 8 月爆发了东南亚金融危机，并且在一些地区发生了严重的针对当地华人的暴乱。国内计算机爱好者怀着一颗爱国之心和对同胞惨遭杀害的悲痛之情，纷纷对这些行为进行抗议。当时黑客代表组织为“绿色兵团”（中国大陆最大最早的民间黑客组织之一）。

- **第 2 代（1998 年～2000 年）**

随着计算机的普及和 Internet 的发展，越来越多的人有机会接触计算机和网络。在第 1 代黑客的影响和指导下，中国出现第 2 代黑客。他们一部分是从事计算机行业的工作者和网络爱好者，另一部分是在校学生。第 2 代黑客的兴起是由 1999 年 5 月 8 日美国轰炸中国驻南斯拉夫大使馆事件引起的，黑客代表组织为“中国黑客联盟”。

- **第 3 代（2000 年至今）**

主要由在校学生组成，其技术水平和文化素质与前两代相差甚远，大都是照搬网上一些由前人总结出来的经验和攻击手法。目前网络上所谓的入侵者也是由这一代组成。

3.2 常见的网络攻击

由于系统脆弱性的客观存在，操作系统、应用软件、硬件设备不可避免地存在一些安全漏洞，网络协议本身的设计也存在一些安全隐患，这些都为攻击者采用非正常手段入侵系统提供了机会。目前，常见的网络攻击包括网站被黑、数据被改或被窃、秘密泄露、非法删除等。

3.2.1 攻击目的

网络安全主要表现在信息的完整性、保密性、可用性、不可否认性和可控性，对于攻击者来讲，就是要通过一切可能的方法和手段来破坏这些安全属性。因此，攻击目的能够表明入侵目的，也是理解攻击者（或称为黑客）的关键。通常多个攻击目的相互共存。

1. 获取保密信息

网络信息的保密性目标是防止未经授权泄露敏感信息。网络中需要保护的信息通常包括重要配置文件、用户账号、注册信息、商业数据（如产品计划）等。通常获取保密信息包括以下几个方面。

- **获取超级用户的权限**

具有超级用户的权限，意味着可以做任何事情，这对于入侵者来讲无疑是一个莫大的诱

惑。在一个局域网中，掌握一台计算机的超级用户权限，也就掌握了整个子网。

❑ **对系统进行非法访问**

一般来讲，计算机系统是不允许其他用户访问的，如一个公司的网络等。因此，必须采取一种非正常的行为来取得系统的访问权限。这种攻击的目的并不一定代表黑客（或攻击者）要做什么，或许只是为访问而攻击。例如，在一个有许多 Windows XP 用户的网络中，常常会有许多用户将自己的文件共享给其他用户使用，于是别人（攻击者）就可以通过攻击来从容地在这些计算机上浏览、寻找自己感兴趣的东西，删除或更换文件等。

❑ **获取文件和传输中的数据**

攻击者的目标就是系统中的重要数据，因此攻击者主要通过登录目标主机，或是使用网络监听进行攻击来获取文件和传输中的数据。

常见的针对信息保密的攻击方法包括使用社会工程学手动骗取用户名和密码、发布免费软件，内含早期计算机信息的木马、搭线窃听、偷看网络传输数据等进行拦截网络信息、使用敏感的无线电接收设备，远距离接收计算机操作者的输入和屏幕显示产生的电磁辐射、将网络重定向，攻击者通过使用一些手段将信息发送端重定向到攻击者所在的计算机，然后再转发给接收者。例如，攻击者伪造某网上银行域名或相似域名，欺骗用户账号和密码。

另外，攻击者使用数据推理，可能从已公开的信息中推测出其他敏感信息。

2．破坏网络信息的完整性

网络信息的完整目标是防止未经授权信息修改，在一些特定的环境中，完整性比保密性更重要。例如，攻击者将一笔电子交易的金额由 100 万改为 1000 万甚至更多，这比泄露交易本身结果更严重。

另外，涂改信息包括对重要文件的修改、更换和删除。其中，删除是一种很恶劣的行为。不真实或者错误的信息都将对用户造成很大的损失。攻击者通常伪装成具有特权的用户来破坏网络信息的完整性。这些方法包括密码猜测、窃取口令、窃听网络连接口令、密钥泄露、中继攻击等。

3．攻击网络的可用性

可用性是指信息可被授权者访问并按需求使用的特性。即保证合法用户对信息和资源的使用不会被不合理地拒绝。

拒绝服务攻击就是针对网络可用性进行的攻击，其方式有多种，如将连接局域网的电缆接地、向渔民服务器发送大量无意义的请求，使得它们无法完成从其他计算机发来的解析请求、制造网络风暴，让网络中充斥着大量的封包，占据网络带宽，延缓网络的传输。

4．改变网络运行的可控性

可控性是指对信息的传播及内容具有控制能力的特性。授权机构可以随时控制信息的机密性，能够对信息实施安全监控。例如，网络蠕虫、垃圾邮件、域名服务器数据破坏等攻击都属于此类攻击。

攻击者使用一些系统工具会被系统日志记录下来，如果直接发给自己的站点也会暴露自己的身份和地址，于是在窃取信息时，攻击者将这些信息和数据发送到一个公开的站点（如

FTP），或者利用电子邮件寄往一个可以取到的地方，以后再从这些地方取走。这样可以很好地隐藏自己。但是，将这些重要信息发往公开的站点也造成了信息的扩散，由于那些公开站点通常会有许多人访问，其他用户也完全可能得到这些信息，并再次扩散出去。

在局域网中，用户被允许访问一些特定资源，而很多访问都不限制。例如，网关对一些站点的访问进行严格控制等。许多用户都有意无意地去尝试尽量获取超出自身权限的访问，于是便寻找管理员在配置中的漏洞，或者使用一些工具来突破系统防线，如特洛伊木马就是一种常用手段。

5. 逃避责任

攻击者为了能够逃避惩罚，往往会通过清除攻击痕迹等方式抵赖攻击行为，或进行责任转嫁，达到陷害他人的目的。攻击者为了攻击的需要，会找出一个中间站点来运行所需要的程序，并且这样也可以避免暴露自己的真实地址。即使被发现了，也只能找到中间站点地址。

另外，假使有一个站点能够访问另一个严格受控的站点或网络，为了攻击这个严格受控的站点或网络，入侵者会借助中间站点主机，对严格受控站点的目标主机进行访问或工具。当造成损失时，责任会转嫁到中间站点主机的管理员身上。

另外，理解攻击目的还有助于人们了解是哪些因素使计算机及其网络成为这些人的目标。是因为系统有价值，还是具有诱惑性？哪种类型的入侵者对系统感兴趣？这些问题的答案可以使安全专家更好地评估对系统的威胁。也有利于针对存在问题制定相应的安全策略。从这个角度来讲通常包括如下 3 个攻击目的。

❑ **挑战**

攻入计算机系统的初始目的是因为这种行为具有挑战性，这也是最常见的黑客攻击目的。在黑客成功进入他人的系统之后，他们就会感觉很有成就感，便会在 Internet 在线聊天室或论坛中的一些专门为此设置的频道或栏目中吹嘘他们的成就。通过对相应频道或栏目的监听表明，黑客通过攻击有难度的系统或大量的系统，或者控制、涂改他们所入侵系统的内容而赢得地位。

挑战的另一个方面不是攻击一个系统的难度，而是成为第一个攻入特定系统的人或攻击的系统数据量最多。有时，黑客会将使他们成功攻击系统时利用的薄弱点消除，以防其他人再次攻击该系统。

这种具有挑战目的的黑客通常是无目标的，也就是说，那些以攻击为乐趣的人并不真正关心他攻击的是哪一个系统。他们一般不会以寻找特定信息或访问为目标，这对安全的意义很有说明性，因为连接 Internet 的所有系统都是潜在的目标。

❑ **贪婪**

在这里将贪婪引申为包括任何以获得钱财、货物、服务或信息的欲望。因此通过识别、抓获黑客并对其进行判罪的难度，来证明这种目的的攻击行为。

如果发现入侵活动，那么大多数用户都会修补导致入侵的薄弱点，清理系统并继续他们的工作。一些用户可能会通知执法机关，但追踪入侵者的工作会因缺少证据、黑客技术水平较高或黑客在没有计算机安全法律国家使用计算机而受到削弱。假设追踪并逮捕了黑客，那么必须将这个案件提交法庭，检察院必须在合理的怀疑之外提供证据证明坐在被告席上的人就是攻入受害的系统并窃取了一些东西的那个人，这是很困难的。

下面看看“熊猫烧香”病毒的案例。据腾讯网 2007 年 2 月份的消息，曾在互联网上引起恐慌的“熊猫烧香”病毒案日前在湖北告破，病毒制造者李某与其他 5 名主要贩卖、传播者落网，这是我国破获的国内首例制作计算机病毒的大案。消息一出，网上舆论一片欢腾。山东威海的王某是“熊猫烧香”病毒的主要购买和传播者之一。他贩卖“熊猫烧香”病毒不足一个月，赚的钱就买了一辆吉普车。被抓获后，22 岁的王某长叹：“这是个比房地产来钱还快的暴利产业！”。

“熊猫烧香”病毒自 2006 年 12 月初开始暴发，到 2007 年 1 月中旬，该病毒变种数已达 90 多种，国内多家门户网站被种植这一病毒，个人用户感染者已经高达几百万。2007 年 1 月 31 日，公安部抽调精干技术力量指导办案。2007 年 2 月 3 日，仙桃警方在武汉市抓获病毒制造者李某。此后 10 天内，王某及其他 4 名涉嫌贩卖传播病毒的骨干分子被缉拿归案。

这个例子展示了关于贪婪的关键点：必须有一种方式能够控制犯罪的消极影响。所以就攻击系统的情况来说，被捕和被判有罪的风险很小，因此偷窃信用卡号、货物或信息的窃贼的潜在收益非常大。贪婪的黑客会寻找可以卖掉或用来获取钱财的特定类型的信息。

这种贪婪的黑客很可能有明确的目标。这时，包含有价值的内容（软件、钱财或信息）的站点是首要目标。

2007 年 2 月国家计算机网络应急技术处理协调中心发布《2006 年网络安全工作报告》公告称，我国网络安全事故同比有大幅度增加，其中，国内政府机构网页篡改事件、国内外商业机构网页被仿冒事件和针对互联网企业拒绝服务攻击事件的影响最为严重。

该报告指出，僵尸网络和木马威胁非常严重，攻击者非法利益目的更加明确、行为更加嚣张，黑客地下产业链基本形成。恶意代码成为黑客入侵用户主机、构建僵尸网络进而窃取用户重要信息并控制受害计算机发起大规模攻击的重要手段。国家计算机网络应急技术处理协调中心每天能发现新的漏洞攻击型恶意代码 96 个，每天捕获次数 3069 次。

国家计算机网络应急技术处理协调中心称，我国互联网用户和信息系统遭受攻击的情况不容乐观。在木马方面，国家计算机网络应急技术处理协调中心抽样发现，2006 年我国大约有 4.5 万个 IP 地址（包含动态 IP）的主机被植入木马，比同期增加 1 倍。

在僵尸网络方面，去年我国有 1000 多万个 IP 地址主机被植入僵尸程序。境外 1.6 万个 IP 对中国的僵尸主机进行控制，主要位于美国、韩国等。

在网页篡改方面，2006 年我国被篡改的网站达到 24477 个，同比增长约 1 倍。其中.gov 网站被篡改数量为 3831 个。

2006 年，与用户密切相关的漏洞有 87 个，同比增长 16%。其中部分漏洞严重威胁互联网运行安全，大多数漏洞对用户的系统造成严重威胁。

2006 年，与安全漏洞关系密切的“零日攻击（漏洞公布当日就出现攻击手段）”现象明显增加。

国家计算机网络应急技术处理协调中心认为，我国公共互联网网络安全令人担忧。未来，在利益驱动下，网络安全事故将更加频繁、隐蔽和复杂。

❑ 恶意

恶意也是黑客攻击的目的之一。在这种情况下，表现为恶作剧或故障破坏，黑客不关心对系统的控制（除了进一步的破坏之外）。相反，黑客打算通过拒绝合法用户使用计算机或者将站点的消息更改为对合法拥有者不利的形式来造成破坏。恶意攻击一般会针对特定目标。

黑客会积极寻找破坏特定站点或机构的方式。

黑客进行故障破坏的潜在理由可能是他（或她）觉得受到了被攻击者的不公平对待或者想通过丑化来达到其他的目的。无论真正的原因是什么，攻击的目的是进行破坏而不获得信息或利益。

3.2.2 攻击分类

十几年前，网络工具还仅局限于破解口令和利用操作系统已知漏洞等有限的几种方法，随着计算机和网络技术的发展网络攻击技术也在不断发展，攻击手段也越来越多。下面基于技术手段的不同对网络攻击进行分类，以便用户能够更多地了解网络的攻击行为，并根据不同的攻击类型采取相应的安全防范措施。

1. 口令窃取

登录一台计算机最容易的方法就是使用正确的口令进入。口令窃取一直是网络安全中的一个重要问题，口令的泄露意味着整个系统的防护已经被瓦解。

攻击者使用最多的攻击方法就是口令猜测，即利用字典或穷举的方法把口令找出来。

2. 缺陷和后门

事实上，目前还没有完美无缺的代码，在系统的某处也许正潜伏着重大的缺陷或者后门，等待人们发现。谁发现并不重要，重要的是谁先发现，是安全专家还是黑客们（攻击者）。

只要本着怀疑一切的态度，从各个方面检查所输入信息的正确性，这些缺陷是可以回避的。例如，如果程序存在固定长度缓冲区，那么就保证它不溢出；如果使用动态内存分配，一定要为内存或文件系统的耗尽作好准备，并且及时释放已分配的内存。

3. 鉴别失败

即使是一个完善的机制在某些特定情况下也会被攻破，因为，如果源计算机不可信，那么基于地址的鉴别也将失效。

一个源地址有效性的验证机制，在某些应用场合（如防火墙筛选伪造的数据包）能够发挥作用，但是黑客可以使用 Portmapper（端口映射器）程序重传某一请求，在这种情况下，服务器最终会受到欺骗，对于这些服务器来讲，报文表面上源于本地，但实际上却源于其他地方。

4. 协议失败

寻找协议漏洞一直在黑客中长盛不衰，在密码学研究领域更是如此。有时是由于密码生成者犯了错误，使得密码过于明了和简单。但更多的情况是由于不同的假设造成的，而证明密码交换的正确性是很困难的事。

5. 信息泄露

信息泄露是指信息被泄露或透漏给某个非授权实体，大多数的协议都会泄露某些信息。

高明的黑客并不需要知道局域网中有哪些计算机，他们只要通过地址空间和端口扫描，就能够找到隐藏的主机和感兴趣的服务。最好的防御方法是配置高性能防火墙，如果黑客们不能够向一台计算机发送数据包，那么该计算机就不容易被入侵。

6. 欺骗攻击

网络欺骗攻击是一种非常专业化的攻击手段，给网络安全管理者带来了严峻的考验。其主要方式包括 IP 欺骗、ARP 欺骗、DNS 欺骗、Web 欺骗、电子邮件欺骗、源路由欺骗（通过指定路由，以假冒身份与其他计算机进行合法通信或发送报文，使受攻击计算机出现错误动作）、非技术类欺骗（利用人与人之间交往，通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的密码）。

7. 拒绝服务

拒绝服务攻击（Denial of Service，DoS）是指攻击者过多地占用系统资源直到系统繁忙、超载而无法处理正常工作，甚至导致被攻击的主机系统崩溃。攻击者的目的很明确，即通过攻击使系统无法继续为合法的用户提供服务。

网络攻击的分类方法很多，如基于攻击效果可以将其分为破坏、泄露和拒绝服务等；还可以将安全性的工具分为被动攻击和主动攻击。其中，被动攻击试图获得或利用系统的信息，但并不会对系统的资源造成破坏，如窃听和检测等；主动攻击则试图破坏系统的资源，并影响系统的正常工作，如拒绝服务等。

3.2.3　网管心得——留后门与清痕迹的防范方法

网络后门是保持对目标主机长久控制的关键策略，通常可以通过建立服务端口和克隆管理员账号来实现。

只要能不通过正常登录进入系统的途径都称为网络后门。后门的好坏取决于被管理员发现的概率。只要是不容易被管理员发现的后门都是好后门。

1. 留后门的防范

通常，入侵者在第一次入侵成功后会在远程主机/服务器内部建立一个备用的管理员账号，以便于更加长久地控制该主机/服务器，这种账号就是最简单的“后门账号”。

另外，还有一种克隆账号，克隆账号就是攻击者（黑客）可以通过将管理员权限复制给一个普通账户。简单地说就是将系统内原有的账号（如 Guest 账号）变成具有管理员权限的账号。克隆账号与直接赋予管理员权限的账号的主要区别在于直接赋予管理员权限的账户，可以使用“命令”或“账号管理”来看出该账号的真实权限，而克隆出来的账号却无法被上述方法直接查出。因此，克隆账号常被入侵者用来当做后门账号。

为了杜绝 Guest 账号的入侵。管理员可以禁用或彻底删除 Guest 账户，但在某些必须使用到 Guest 账号的情况下，就需要通过其他途径来做好防范工作。首先需要给 Guest 账号设置一个强壮的密码，然后再详细设置 Guest 账号对物理路径的访问权限（注意磁盘必须是 NTFS 分区）。



密码设置尽可能使用字母数字混排，单纯的英文或者数字很容易穷举。将常用的密码设置成不同的，防止被人查出一个，连带到重要密码。重要密码最好经常更换。

另外，还需要注意对如下几个方面的防范。

- 实施用户账户封锁策略。
- 为系统和网络的审计实施有效的审计策略。
- 正确配置用户权限将阻止恶意系统用户访问其他用户文件。
- 保护系统文件和目录权限，可以有效地保护日志文件，从而使未授权用户不能访问这些文件夹。
- 限制空连接，保护共享文件，可以通过启用防火墙监视网络连接情况。
- 禁用不必要的服务。



IPC$（Internet Process Connection）是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。利用 IPC$连接者不仅可以与目标主机建立一个空的连接而无需用户名与密码还可以得到目标主机上的用户列表。

2. 清痕迹防范

为了方便用户对计算机的使用，Windows 自带了一些功能（如自动记录功能），但是这些功能在给用户带来方便的同时，也给攻击者（黑客）的入侵带来了方便，他们往往能够通过用户曾经执行过的操作痕迹来找到入侵系统的方法及所需的信息。

为了避免这些使用痕迹带来的安全隐患，建议用户在使用计算机的过程中注意清理痕迹，这通常包括如下几个方面的内容。

❑ 彻底删除文件

首先，应从系统中清除那些肯定不用的文件（丢弃到回收站中的所有垃圾文件）。当然，用户也可以在任何想起的时候将回收站清空。但是更好的方法是关闭回收站的回收功能。要彻底地一次删除文件，需要右击【回收站】图标，执行【属性】命令，在弹出的对话框中，选中【所有驱动器均使用同一设置】单选按钮，并启用【删除时不将文件移入回收站，而是彻底删除】复选框。然后，单击【确定】按钮，如图 3-1 所示。

❑ 删除文件记录

即使窥探者无法直接浏览文档内容，他们也能够通过在 Microsoft Word 或 Excel 的【文件】菜单中查看到用户最近使用过哪些文件来了解用户的工作情况。在该列表中甚至列出了最近被删除的文件，因此最好关闭该功能。其方法为：在 Word 或 Excel 中，执行【Office 按钮】|【Word 选项】命令，在打开的对话框中，选择【高级】选项，并在右侧【显示】窗格中，将【显示此数目的“最近使用的文档”】文本框内数字修改为“0”，如图 3-2 所示。然后，单击【确

定】按钮。

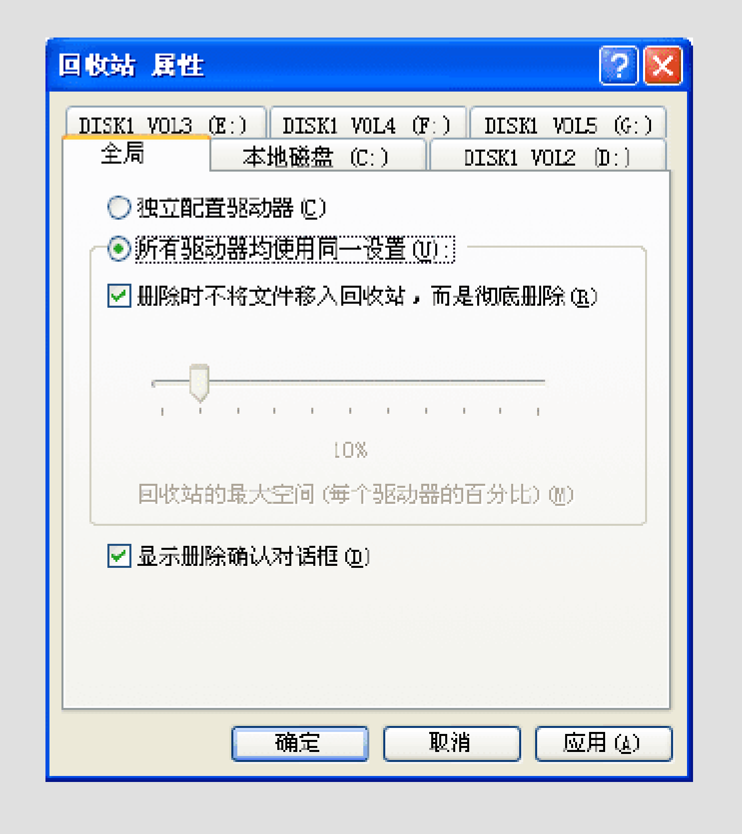


图 3-1　回收站属性

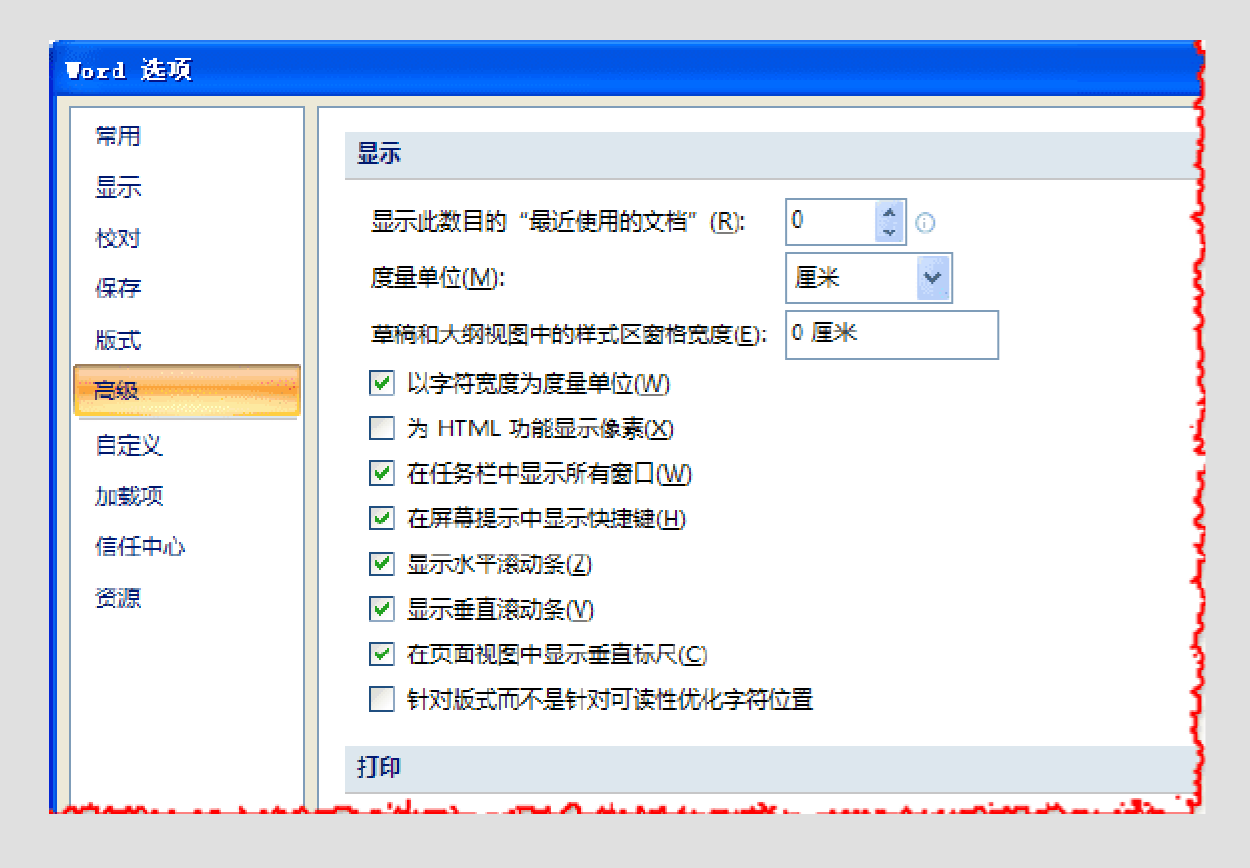


图 3-2　修改最近使用文档数

❑ 隐藏文档内容

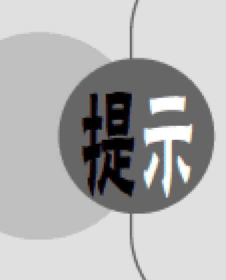
在 Windows 系统中，通过执行【开始】|【文档】命令，可以查看到用户所使用过文档的记录，这使得他人能够非常轻松地浏览该用户的工作文件或个人文档。要清空该列表，需要用户执行【开始】|【设置】|【任务栏和「开始」菜单】命令，在弹出的对话框中切换到【「开始」菜单】选项卡，并单击【自定义】按钮。然后，在弹出的对话框中单击【清除】按钮，如图 3-3 所示。

❑ 清除临时文件

Microsoft Word 和其他应用程序通常会临时保存用户的工作结果，以防止意外情况造成损失。即使用户没有保存正在处理的文件，许多程序也会保存已被删除、移动和复制的文本。用户应当定期删除各种应用程序在 WINDOWSTEMP 文件夹中存储的临时文件，以清除上述这些零散的文本。另外，还应删除其子目录（如 FAX 和 WORDXX 目录）中相应的所有文件。虽然很多文件的扩展名为 TMP，但它们其实是完整的 DOC 文件、HTML 文件，甚至是图像文件。

❑ 清除网页访问历史记录

浏览器也是需要保护的另一重要部分。目前，大多数用户都使用 Windows 系列操作系统，Windows 自带 Internet Explorer 浏览器，它会把用户访问过的所有对象都列出清单保存下来，其中包括浏览过的网页、进行过的查询以及曾输入的数据等内容。通常，Internet Explorer 将网页访问历史记录保存在按周划分或按网址划分的文件夹中。用户可以单个地删除各个“地址（URL）”，但最快的方法是删除整个文件夹，清除全部历史记录，其方法是：在 Internet Explorer 中，执行【工具】|【Internet 选项】命令，在打开的对话框中单击【清除历史记录】按钮。



Internet Explorer 会在硬盘中缓存用户最近访问过的网页。当用户再次访问这些网页时，高速缓存信息能够加快网页的访问速度，但这也向窥探者揭开了用户的秘密。要清除这些高速缓存信息，只需用户在此单击【删除文件】按钮即可。





图 3-3　清除文档记录　　　　图 3-4　清除网页历史记录

3.3　木马攻击与分析

木马攻击是黑客最常用的攻击方法。木马的危害性在于它对计算机系统强大的控制和破坏能力（如窃取密码、控制操作系统、进行文件操作等），一台计算机一旦被一个功能强大的木马入侵，攻击者就可以像操作自己的计算机一样控制该计算机，并远程监控这台计算机上的所有操作。

3.3.1　木马背景介绍

“木马”一词来自于“特洛伊木马”，英文名称为“Trojan horse”。据说该名称来源于古希腊传说，特洛伊王子帕里斯访问希腊，诱走了王后海伦，希腊人因此远征特洛伊。围攻 9 年后仍未攻下，到了第 10 年，希腊将领奥德修斯出此一计，就是把一批勇士埋伏在一匹巨大的木马腹内，放在城外后，大部队则佯装退兵。特洛伊人以为希腊敌兵已退，就把木马作为战利品搬入城中。全城饮酒狂欢，到了夜间，全城军民进入梦乡，而埋伏在木马中的勇士们跳了出来，并打开城门及四处纵火，城外希腊将士一拥而入，部队里应外合，攻下了特洛伊城池。后世称这只大木马为“特洛伊木马”。后来，人们在写文章时，就常用“特洛伊木马”这一典故用来比喻在敌方营垒内埋下伏兵里应外合的活动。而黑客程序也借用其名，有“一经潜入，后患无穷”之意。

3.3.2　木马概述

木马是一种可以驻留在对方服务器系统中的一种程序。木马程序一般由服务器端程序和客户端程序两部分构成。驻留在对方服务器的称为木马的服务器端，远程的可以连接到木马服务器的程序称为木马客户端。木马的功能是通过客户端可以操纵服务器，进而操纵对方的计算机。

1. 木马工作原理

目前木马入侵的主要途径还是先通过一定的方法把木马执行文件发送到被攻击者的计算机中，利用的途径有邮件附件、下载软件等，然后通过一定的提示故意误导被攻击者打开执行程序，如故意谎称这个木马执行文件，是用户朋友送的贺卡，可能打开这个文件后，确实有贺卡的画面出现，但这时木马可能已经悄悄在计算机的后台中运行。

一般的木马执行文件非常小，大部分都是几 KB 到几十 KB，如果把木马捆绑到其他正常文件上，用户将很难发现，所以，有一些网站提供的软件下载往往是捆绑了木马文件的，用户执行这些下载的文件，同时也运行了木马。

木马也可以通过 Script、ActiveX 及 ASP、CGI 交互脚本的方式植入，由于微软的浏览器在执行 Script 脚本时存在一些漏洞。攻击者可以利用这些漏洞传播病毒和木马，甚至直接对浏览者的计算机文件进行操作控制。如前不久曾出现一个利用微软 Script 脚本漏洞对浏览者硬盘进行格式化的 HTML 页面。如果攻击者有办法把木马执行文件下载到攻击主机的一个可执行 WWW 目录下，他可以通过编制 CGI 程序在被攻击计算机上执行木马程序。此外，木马还可以利用系统的一些漏洞进行植入，如微软著名的 US 服务器溢出漏洞，通过一个 IISHACK 攻击程序即可使 IIS 服务器崩溃，并且同时攻击服务器，通过执行远程木马来控制执行文件。

当服务端程序在被感染的机器上成功运行以后，攻击者就可以使用客户端与服务端建立连接，并进一步控制被感染的机器。在客户端和服务端通信协议的选择上，绝大多数木马使用的是 TCP/IP 协议，但是也有一些木马由于特殊的原因，使用 UDP 协议进行通信。当服务端在被感染机器上运行以后，它一方面尽量把自己隐藏在计算机的某个角落里面，以防被用户发现；同时监听某个特定的端口，等待客户端与其连接；另外为了使下次用户重启计算机时仍然能正常工作。木马程序一般会通过修改注册表或者其他的方法让自己成为自启动程序。

2. 木马特性

木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段来隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，也很难消除。通常包括如下隐藏方式。

❑ **在任务栏中隐藏**

这是最基本的隐藏方式。如果在 Windows 的任务栏里出现一个莫名其妙的图标，那么用户马上会明白是怎么回事。因此，黑客会设法不让此事发生。通过编程语言来实现在任务栏中的隐藏是很容易实现的。以 VB 为例，在 VB 中，只要把 from 的 Visible 属性设置为 False，ShowInTaskBar 设为 False，那么程序就不会在任务栏里出现了。

❑ **在任务管理器中隐藏**

查看正在运行的进程最简单的方法就是按 Ctrl+Alt+Del 键，在打开的【任务管理器】窗口中查看。如果用户可以查看到一个木马程序在运行，那么这肯定不是什么好木马。因此，木马会千方百计地伪装自己，使自己不出现在任务管理器中。木马只要把自己设为“系统服务”就可以轻松地骗过用户。因此，希望通过按 Ctrl+Alt+Del 键发现木马是不大现实的。

❑ 端口

一台计算机有 65536 个端口，用户通常不注意这么多的端口，但是木马却很注意这些端口。如果人们稍微留意一下，不难发现大多数木马使用的端口都在 1024 以上，而且呈越来越大的趋势。当然也有占用 1024 以下端口的木马，但这些端口是常用端口，占用这些端口可能会造成系统不正常，这样的话，木马就会很容易暴露。也许用户知道一些木马占用的端口，或许会经常扫描这些端口，但现在的木马都提供端口修改功能，用户通常没有时间扫描 65536 个端口。

❑ 隐藏通信

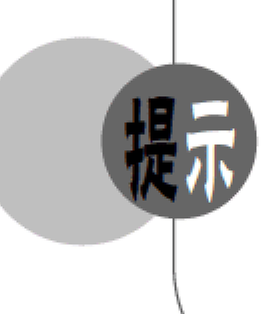
隐藏通信也是木马经常采用的手段之一。任何木马运行后都要和攻击者进行通信连接，或者即时连接（如攻击者通过客户端直接或间接接入被植入木马的计算机），或者通过间接通信。如通过电子邮件的方式，木马把侵入主机的敏感信息发送给攻击者。现在大部分木马一般在占领主机后会在 1024 以上不易发现的高端口上驻留；有一些木马会选择一些常用的端口，如 80、23，有一种非常先进的木马还可以做到在占领 HTTP 端口（80）后，收到正常的 HTTP 请求仍然把它交于 Web 服务器处理，只有收到一些特殊约定的数据包后，才调用木马程序。

❑ 隐藏加载方式

木马加载的方式可以说千奇百怪。但殊途同归，那就是使用户运行木马的服务端程序。如果木马不做任何伪装，那么用户通常是不会运行该木马的。而随着网站互动性技术的不断进步，越来越多的东西可以成为木马的传播介质，Java Script、VBScript、ActiveX.XLM 等，几乎 WWW 每一个新功能都会导致木马的快速进化。

❑ 最新隐身技术

这是一种更新、更隐蔽的方法。通过修改虚拟设备驱动程序（VXD）或修改动态连接库（DLL）来加载木马。与一般方法不同，这种方法基本上摆脱了原有木马的工作模式—监听端口，而采用替代系统功能的方法（改写 VXD 或 DLL 文件），木马会将修改后的 DLL 替换成系统已知的 DLL 文件，并对所有的函数调用进行过滤。进行常用的调用，使用函数转发器直接转发给被替换的系统 DLL 文件，进行一些相应的操作。实际上，这样的事先约定好的特殊情况，DLL 会执行一般只是使用 DLL 进行监听，一旦发现控制端的请求就激活自身，绑在一个进程上进行正常的木马操作。这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到它。在往常运行时，木马几乎没有任何症状，当木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运作。



实际上，由于大量木马对 DLL 文件的使用已经危害到了 Windows 操作系统的安全和稳定性，微软公司已经开始使用 DLL 数字签名、校验技术来加强系统的安全性，因此，木马使用 DLL 文件的时代很快会减少。取代它的将会是强行嵌入代码技术（插入 DLL、挂接 API、进程的动态替换等），但是这种技术对于编写者的汇编功底要求很高，因为涉及大量硬编码的机器指令，并不是一般的木马编写者可以涉足的。

另外，非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权

限，包括修改文件，修改注册表，控制鼠标、键盘等，这些权力并不是服务端赋予的，而是通过木马程序窃取的。

木马除具有隐蔽性和非授权特性之外，还包括如下特性。

❑ **具有自动运行性**

木马为了控制服务端，必须在系统启动时即跟随启动，所以它必须潜入在计算机的启动配置文件中，如 win.ini、system.ini、winstart.bat 以及启动组等。

❑ **具有未公开并且可能产生危险后果功能的程序**

❑ **具备自动恢复功能**

现在很多的木马程序中的功能模块不再由单一的文件组成，而是具有多重备份，可以相互恢复。当用户删除了其中的一个，以为万事大吉又运行其他程序的时候，谁知它又悄然出现。所以很难全部消除。

❑ **能自动打开特别的端口**

木马程序潜入用户的计算机主要不是为了破坏系统本身，而是为了获取用户系统中有用的信息，当用户上网时能与远程客户进行通信，这样木马程序就会用服务器客户端的通信手段把信息发送给黑客，以便黑客们控制用户的计算机，或实施进一步的入侵企图。根据 TCP/IP 协议，每台计算机可以有 256 乘以 256 个端口，即端口号范围为 0～65535，但常用的只有少数几个，木马经常利用那些不常用的端口进行连接。

❑ **功能的特殊性**

通常的木马功能都是十分特殊的，除了普通的文件操作以外，有些木马具有搜索缓存（cache）中的口令、设置口令、扫描目标计算机的 IP 地址、进行键盘记录、远程注册表的操作以及锁定鼠标等功能。

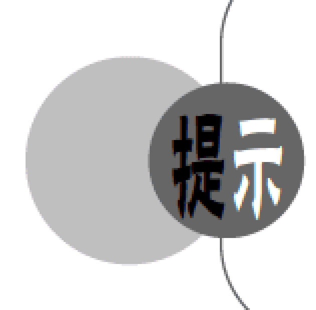
3.3.3　木马的分类

木马程序诞生至今，已经产生了多种类型，且大多数木马的功能不是单一的，而是多种功能的集合，甚至有些功能从未公开。因此，给木马程序进行分类、了解木马的危害对于计算机使用者来说是很必要的。

1. 远程控制型

远程控制木马是数量最多，危害最大，同时也是知名度最高的一种木马，它可以让攻击者完全控制被感染的计算机，攻击者可以利用它完成一些甚至连计算机使用者本身都不能顺利进行的操作，其危害之大实在不容小觑。由于要达到远程控制的目的，该类型木马往往集成了其他木马的功能。使其在被感染的计算机上为所欲为，可以任意访问文件，得到用户的私人信息甚至包括信用卡，银行账号等至关重要的信息。

例如，大名鼎鼎的木马“冰河”就是一个远程访问型特洛伊木马。这类木马使用起来非常简单。只需有人运行服务端，攻击者就可以得到受害人的 IP 地址，就会访问到他们的计算机。远程访问型木马的普遍特征包括键盘记录、上传和下载功能、注册表操作、限制系统功能等。



这种远程控制也可以用于正当用途，如在学校，教师可以用来监控学生在计算机上所进行的操作。另外，远程访问型木马会在目标计算机中打开一个端口，而且有些木马还可以改变端口、设置密码连接等，其目的只是为了保证仅有黑客自己能够控制该木马。

2. 密码发送型

在信息安全日益重要的今天。密码无疑是通向重要信息的一把极其有用的钥匙，只要掌握了对方的密码，从很大程度上说，就可以无所顾忌地得到对方的很多信息。而密码发送型木马正是专门为了盗取被感染计算机上的密码而编写的，木马一旦被执行，就会自动搜索内存，缓存（Cache），临时文件夹以及各种敏感密码文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱，从而达到获取密码的目的。

这类木马大多使用 25 号端口发送 E-mail。大多数这类的特洛伊木马不会在每次 Windows 重启时启动。这种特洛伊木马的目的是找到所有的隐藏密码并且在受害者不知道的情况下把它们发送到指定的信箱。

3. 键盘记录型

这种特洛伊木马是非常简单的。它们只做一件事情，就是记录受害者计算机的键盘敲击动作并且在 LOG 文件里查找密码。

另外，这种特洛伊木马会随着 Windows 的启动而启动。它们有在线和离线记录这样的选项，顾名思义，它们分别记录用户在线和离线状态下敲击键盘时的按键情况。也就是说用户按过什么键，都会通过电子邮件将记录下的信息发送给相应的攻击者，造成用户信息的泄露。

4. DoS 攻击型

随着 DoS 攻击越来越广泛的应用，被用作 DoS 攻击的木马也越来越流行。当攻击者入侵了一台计算机，给它种上 DoS 攻击木马，那么日后这台计算机就成为攻击者进行 DoS 攻击最得力的助手了。攻击者控制的傀儡主机数量越多，它所发动 DoS 攻击取得成功的几率就越大。所以，这种木马的危害不是体现在被感染计算机上，而是体现在攻击者可以利用它来攻击一台又一台的计算机，给网络带来很大的伤害和损失。

还有一种类似 DoS 的木马叫做邮件炸弹木马，一旦计算机被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方计算机瘫痪，不能接收邮件为止。

5. 代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的傀儡主机种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用 Telnet、ICQ（QQ）、IRC（因特网中继聊天）等程序，从而隐蔽自己的踪迹。

6. FTP 木马

这种木马可能是最简单和最古老的木马了，它的唯一功能就是打开 FTP 端口（21），等待用户连接。现在新 FTP 木马还增加了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。

7. 程序杀手木马

上面的木马功能虽然形形色色，不过到了对方计算机上要发挥自己的作用，还要通过防木马软件检测这一关才行。常见的防木马软件有 Norton Anti-Virus 等。程序杀手木马的功能就是关闭对方计算机上运行的这类防木马软件，让其他的木马更好地发挥作用。

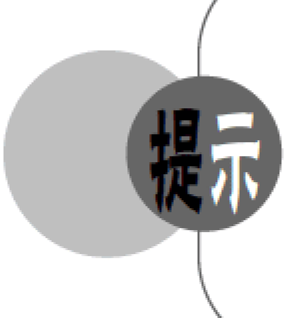
8. 反弹端口型木马

木马开发者在分析了防火墙的特性后发现：防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。于是，与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线立即弹出端口主动连接控制端打开的主动端口。

为了隐蔽起见，控制端的被动端口一般位于 80 端口，这样，即使用户使用端口扫描软件检查自己的端口时，会发现类似 TCP User IP：1026 Controller IP：80 ESTABLISHEN 的情况，稍微疏忽一点，就会以为是自己在浏览网页，因为浏览器就是使用 80 端口，如最早的“网络神偷（Nethief）”木马等。

9. 破坏性质的木马

这种木马唯一的功能就是破坏被感染计算机的文件系统，使其遭受系统崩溃或者重要数据丢失的巨大损失。从这一点上来说，它和病毒很相像。不过，这种木马的激活是由攻击者控制的，并且传播能力也比病毒逊色很多。



代理木马和程序杀手木马这两种类型的木马实际上是其他类型的木马可能具有的功能，如很多远程访问型木马都可以使用代理服务器的方式来连接被控制计算机，而且会首先检查对方是不是开启了防火墙，如果有，则关闭防火墙进程，这样有利于黑客隐藏身份，从而实现远程控制。

3.3.4 网管心得——木马的发展

木马也叫黑客程序或后门病毒，属于文件型病毒的一种。随着计算机网络技术的发展，黑客技术也在不断进步，为了更好地实现攻击目的，攻击者所编制的木马程序功能也更加强大，由木马的特点及其危害性就可以得出木马的发展阶段。

1. 第 1 代木马——伪装型病毒

这种病毒通过伪装成一个合法性程序来诱骗用户上当。例如，世界上第一个计算机木马

是在 1986 年出现的 PC-Write 木马，它可以伪装成共享软件 PC-Write 的 2.72 版本（事实上，编写 PC-Write 的 Quicksoft 公司从未发行过 2.72 版本），一旦用户信以为真运行该木马程序，那么他的计算机硬盘就被格式化。

另外，还有一种伪装登录界面的木马程序，当用户将自己的用户 ID 和密码输入一个和正常的登录界面一模一样的伪登录界面之后，木马程序一方面会保存该用户的 ID 和密码，另一方面会提示用户密码错误，令用户重新输入登录名和密码，当用户第二次登录时，就已经成为木马的牺牲品。此时的第一代木马还不具备传染特征。

2. 第 2 代木马——AIDS 型木马

继 PC-Write 之后，1989 年出现了 AIDS 木马。由于当时很少有人使用电子邮件，所以 AIDS 的作者就利用现实生活中的邮件进行散播，即给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称是因为软盘中包含有 AIDS 和 HIV 疾病的药品、价格、预防措施等相关信息。软盘中的木马程序在被用户运行后，虽然不会破坏数据，但会将硬盘加密锁死，然后提示受感染用户花钱解决该问题。可以说第 2 代木马已具备传播特征（尽管通过传统的邮递方式）。

3. 第 3 代木马——网络传播型木马

随着 Internet 的普及，第 3 代木马不仅兼备伪装和传播两种特征，而且还结合 TCP/IP 网络技术四处泛滥。同时第 3 代木马还有如下新的特征。

- **添加了“后门”功能**

后门就是一种可以为计算机系统秘密开启访问入口的程序。一旦被安装，这些程序就能够使攻击者绕过安全程序进入系统。该功能的目的就是收集系统中的重要信息，例如，财务报告、口令及信用卡号等。此外，攻击者还可以利用后门控制系统，使之成为攻击其他计算机的帮凶。由于后门是隐藏在系统背后运行的，因此很难被检测到。它们不像病毒和蠕虫那样通过消耗内存而引起注意。

- **添加了击键记录功能**

该功能主要是记录用户所有的击键内容然后形成击键记录的日志文件发送给恶意用户。恶意用户可以从中找到用户名、口令以及信用卡号等用户信息。这一代木马比较有名的有国外的 BO2000（Back Orifice）和国内的冰河木马。它们有如下共同特点：基于网络的客户端/服务器应用程序。具有搜集信息、执行系统命令、重新设置机器、重新定向等功能。当木马程序攻击得手后，计算机就完全成为黑客控制的傀儡主机，黑客成了超级用户，用户的所有计算机操作不但没有任何秘密而言，而且黑客可以远程控制傀儡主机对其他主机发动攻击，这时候被俘获的傀儡主机成了黑客进行进一步攻击的挡箭牌和跳板。

3.4 木马的攻击防护技术

只要感染木马，就有可能遭到破坏。遭到破坏的类型包括系统瘫痪、数据被窃取等，木马成为入侵者手中的杀手锏，然而接踵而至的杀毒软件使得木马毫无藏身之地。

木马被杀毒软件的查杀使得入侵者不敢再轻易地使用这些程序，这对于管理员来说是好事，但对于入侵者是一件坏事，面对杀毒软件，入侵者并不是毫无办法，他们可以通过对木马进行修改，使之逃过杀毒软件的查杀。因此，并不是经过杀毒软件扫描的程序就一定不是木马。

3.4.1　常见木马的应用

木马在真正的黑客看来只是一种初级的工具，往往不屑于使用，而对于一些初级黑客、甚至是不算黑客的“黑客”来讲，却是最好的攻击别人、获取密码的工具，因为，这种黑客工具对普通用户的危害极大。

常见的简单的木马有早期的 NetBus 远程控制、“冰河”木马、PCAnyWhere 远程控制及近期的灰鸽子等。其中，冰河可以说是最优秀的国产木马程序之一，同时也是被使用最多的一种木马。

本节就以“冰河 V8.4”为例，介绍“冰河”木马的使用方法。“冰河”木马包括两个程序文件，一个是服务器端程序，一个是客户端程序，图 3-5 所示为“冰河 V8.4”的文件列表内容。

在“冰河 V8.4”木马文件列表中，G_SERVER.exe 文件是服务器端程序，即被监控端后台监控程序（运行一次即自动安装，可任意改名）；G_CLIENT.exe 文件是客户端程序，即监控端执行程序，用于监控远程计算机和配置服务器程序。将 G_SERVER.exe 文件在远程计算机上执行后，通过 G_CLIENT.exe 文件就可以来控制远程服务器。

要使用“冰河”木马，首先需要用户通过客户端对服务器端进行配置，运行客户端 G_CLIENT.exe 程序，在打开的客户端主界面中，单击【设置】菜单，并执行【配置服务器程序】命令，如图 3-6 所示。



图 3-5　“冰河 V8.4”的文件列表



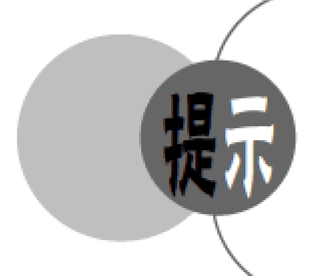
图 3-6　“冰河”客户端主界面



7620 端口是冰河木马默认打开的端口，黑客在设置时有时也会修改这个端口。另外，其他木马可能是使用其他端口，扫描时需扫描相应端口。

在【服务器配置】窗口中，首先单击【浏览】按钮选择待配置文件，然后设置服务器端

的安装路径，更改服务器端文件名，设置访问口令、进程名称、监听端口等内容，如图 3-7 所示。



用户可以根据自己的需要在【提示信息】文本框中输入一些信息。例如，蓄意欺骗对方该程序为错误程序时，就可以输入“程序出错，缺少必须的.dll 文件！”等信息。

选择【自我保护】选项卡，在该选项卡页面，可以设置是否写入注册表的启动项，以便冰河在开机时自动加载以及是否关联文件，以便被删除后再打开相关文件时自动恢复，图 3-8 所示为默认设置。

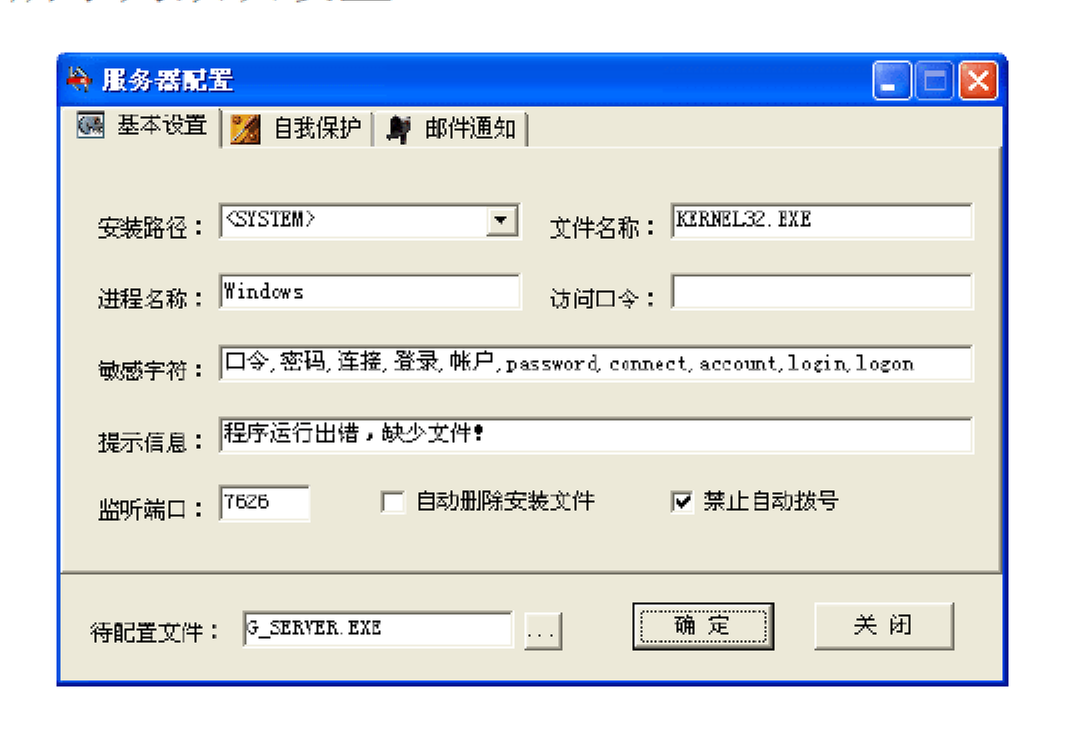


图 3-7　基本设置

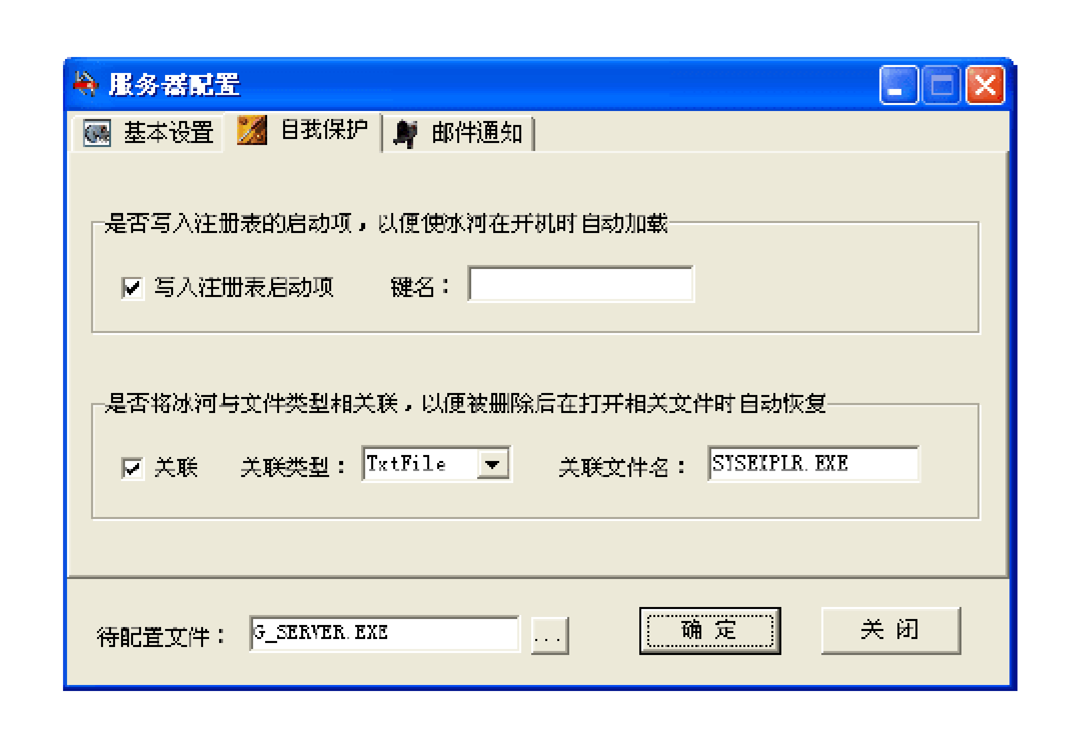


图 3-8　自我保护

选择【邮件通知】选项卡，在该选项卡页面，可以设置将对方计算机系统信息、开机口令、共享资源信息等发送到指定邮箱，设置完成后，单击【确定】按钮即可，如图 3-9 所示。

服务器端设置完成之后，就可以将这个新配置的程序即 G_SERVER.exe 发送给对方计算机，并诱骗对方运行，当用户运行之后，攻击者即可实施远程控制计划。

1. 扫描端口

在开始使用冰河之前，可以利用冰河客户端自带的扫描功能扫描开放了 7626 端口的主机。单击【文件】菜单并执行【自动搜索】命令，或者单击工具栏中的【自动搜索】按钮，如图 3-10 所示。

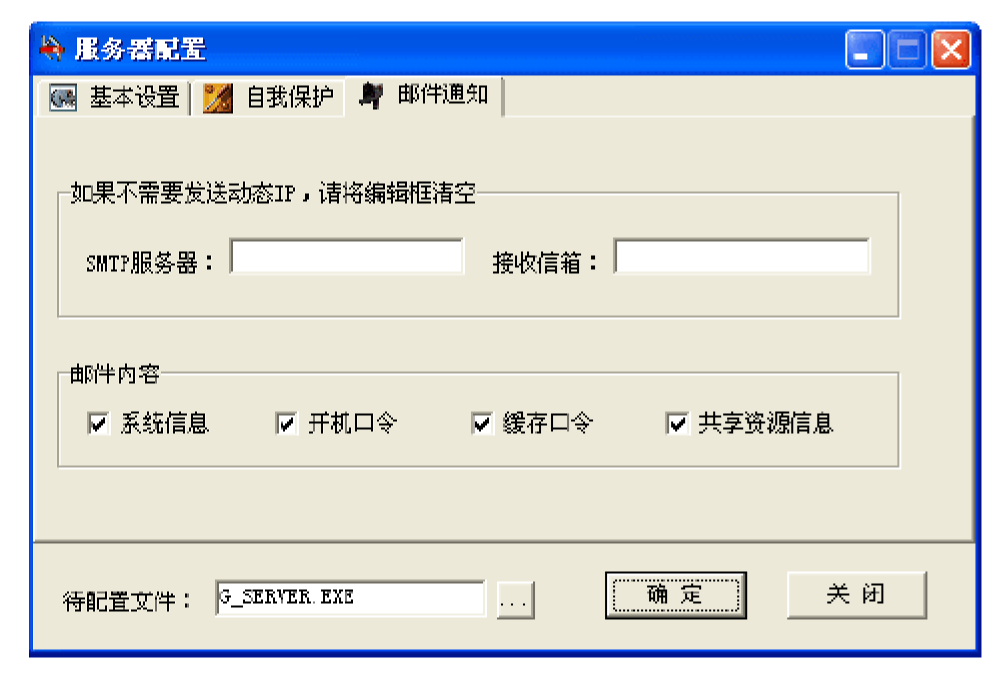


图 3-9　邮件通知



图 3-10　自动搜索

在弹出的【搜索计算机】窗口中，用户可以设置起始域地址、终止地址数等信息，如设置起始域为“192.168.0”，并单击【开始搜索】按钮，即可在【搜索结果】列表中查看搜索到的计算机，如图 3-11 所示。

提示　“冰河”木马自带的搜索功能会使计算机运行速度变慢，功能也较弱，用户可以使用专用的扫描工具（如 X-way 等）来扫描开放了 7626 端口的计算机。

2. 进行远程控制

当使用“冰河”扫描出开放了 7626 端口的计算机后，就可以对该计算机进行远程控制。

首先，运行“冰河”客户端程序，单击【文件】菜单并执行【添加主机】命令，或是单击工具栏中的按钮，如图 3-12 所示。



图 3-11　搜索计算机



图 3-12　添加主机

在弹出的对话框中，输入搜索到的计算机 IP 地址，单击【确定】按钮，如图 3-13 所示。如果出现“无法与主机连接”、“口令有误”等提示信息就放弃，初始密码应该为空，如果出现“口令有误”则表明该计算机已经被其他人完全控制。

当连接成功后，在“冰河”木马主界面中，展开搜索到的 IP 地址节点，如 192.168.0.5，并选择打开“C:”，此时，可以查看到许多文件夹，如图 3-14 所示，此时表明已经成功入侵对方计算机。

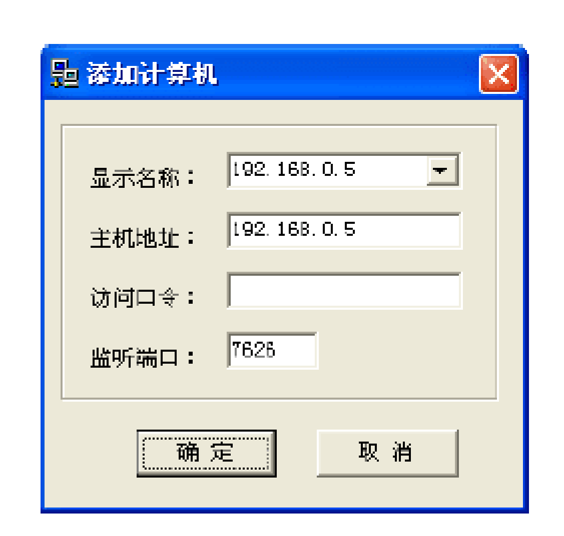


图 3-13　输入计算机 IP 地址

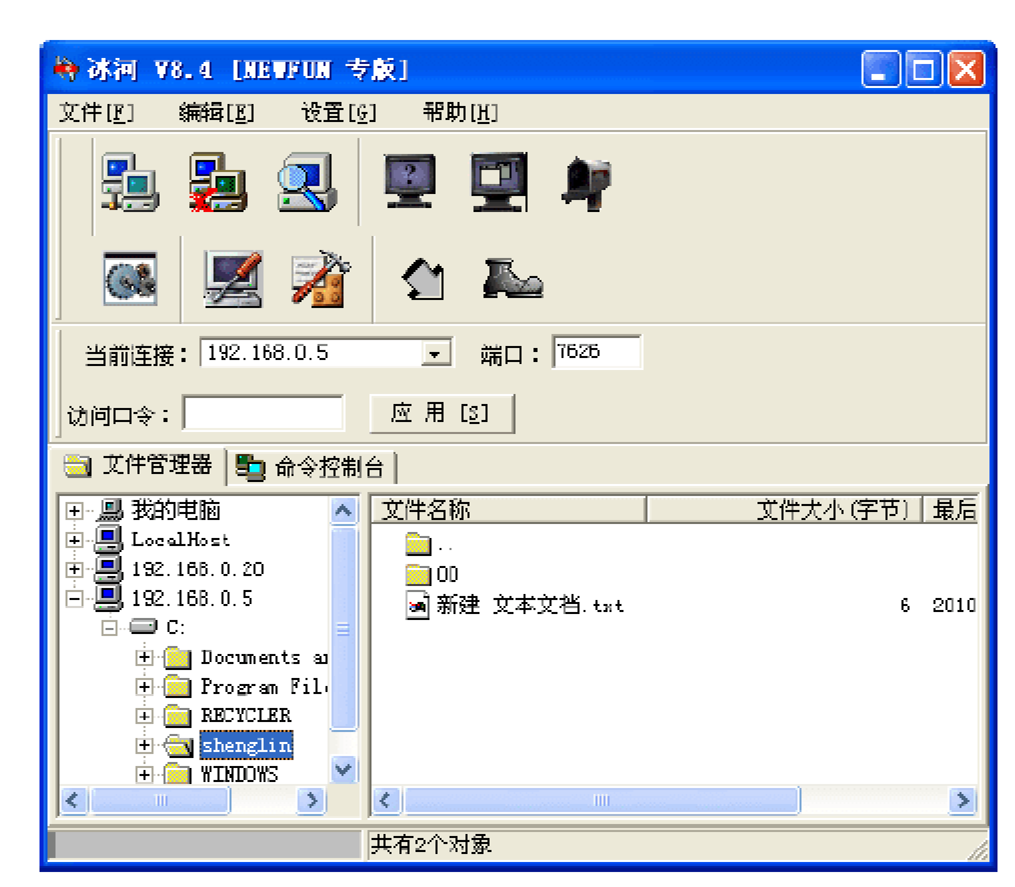


图 3-14　查看对方计算机文件

在文件管理区，攻击者可以对文件、程序等进行上传、下载、删除、远程打开等多项操作，如要这样做，只需要右击文件或程序并执行相应的命令即可，如图 3-15 所示。

接下来，还可以进行其他操作，如选择【命令控制台】选项卡，在该页面，展开【口令类命令】节点，并选择【系统信息及口令】选项，则在右侧窗格中就可以查看到对方计算机的系统信息，如图 3-16 所示。当然，还可以选择其他选项，并进行与之相对应的操作。




图 3-15　下载文件



图 3-16　查看系统信息

另外，木马程序在国内外有多种，原理和功能基本上与“冰河”相似，只是可能有的功能比较强大，有的功能比较简单而已。但由于目前杀毒软件基本可以查杀大多数著名的木马程序，因此知名的木马程序一般不适合用作网络后门程序。

3.4.2　木马的加壳与脱壳

给程序加壳，包括加密壳和压缩壳两种方法。程序一旦被加壳保护后，如果不使用与此相应的脱壳软件进行脱壳处理，那么一些反汇编程序是不能正确读取到其真正的代码的。这样，就能保护程序不会被破解。同样，木马程序一旦经过加壳保护，反病毒软件如果不具有该程序脱壳的功能，那么就不可能识别出它，因此可以说木马加壳达到了隐藏自身的目的。

脱壳是与加壳相反的过程，目的是把加壳后的程序恢复成毫无包装的可执行代码，这样未授权者便可对其进行修改。脱壳的过程与加壳的操作类似，但是对于不同的加壳软件，需要使用不同的脱壳软件。入侵者只要知道目标程序使用的是哪种加壳软件进行加壳的，然后，在使用对应的脱壳软件进行脱壳处理即可。简单地说加壳与脱壳就相当于加密和解密。

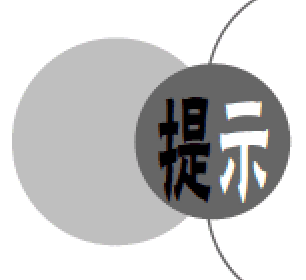
目前，通过 Aspack 或 UPX 给木马加壳是非常容易的。例如，灰鸽子远程控制软件本身就具有 UPX 加壳功能。但是，这些常见的加壳软件的加壳方式已经被杀毒软件研究透彻，加上一些杀毒软件（如卡巴斯基）已经具有对常见木马的脱壳功能。因此，一些攻击者通常会使用一些不常用的加壳软件来对木马程序进行加壳处理。这些不常用的加壳软件，一般都会在一些国外的安全类网站当中找到，其中比较常用的有 Private exe Protector 软件，它原本是

一个非常好用的程序保护软件，但同样也可以用来保护木马。而且，对木马进行加壳，往往还会加多重壳，以进一步增加被人们识别出来的难度，但加多重壳要比加单一的壳要复杂得多。

程序加壳只是对木马的程序文件进行了保护而已，且有时加壳会损坏木马的一些功能，而且，单独使用加壳保护木马是达不到理想的保护效果的。因此，攻击者在对木马加壳保护之前，还会对它使用如程序加密之类的处理工作。

由于对木马进行加壳保护只对木马文件有效，因此，对于已经加载到内存中的木马程序段，木马在运行时已经自动进行脱壳处理，也就失去了保护作用，这样就可以通过使用对内存进行检测的方式来查杀木马。

目前，已经有许多杀毒软件具有了内存查杀的功能，如瑞星等。但是，一些木马的程序在加载到内存之前，会先被它的壳所控制，而这些壳会通过一些手段来终止用户系统中所运行的安全软件的进程，然后再完全将木马程序加载到内存中运行，这样就能躲避被内存查杀的危险。此时，就只能靠用户自己使用一些脱壳软件来对系统中可疑的文件进行查壳和脱壳处理后再查杀。



PEID 和 PESCAN 是两个常用的查看程序加壳情况的软件，对于普通的用户，使用超级巡警虚拟自动脱壳机就能够很好地解决这些问题。同样，使用主动防御功能的安全软件也可以检测到这种类型的木马。

3.4.3 网管心得——安全解决方案

木马程序具有不需要服务端用户的允许即可获得系统的使用权，同时具有体积小、易在网络上传播、运行隐蔽不易被用户察觉的特征。但它还是会表现出如下一些症状。

- 计算机反应速度明显降低。
- 硬盘在不停地读/写。
- 鼠标和键盘使用不灵。
- 窗口关闭或打开。
- 网络传输指示灯一直在闪烁。

为了避免木马的危害，人们也在不断地研究防范措施，目前，对于木马的安全解决方案主要包括如下几个方面。

1. 安装反病毒软件

用户在上网时应该时刻打开杀毒软件，目前大多数反病毒工具软件几乎都可以检测到所有的特洛伊木马，但用户需要注意及时更新反病毒软件。

2. 安装木马专杀软件

反病毒软件虽然能够检测出木马，但却不能将其从计算机中删除。因此，还需要用户安装诸如 TROJIAREMOVER 之类的软件，将木马删除。

3. 安装个人防火墙

如果计算机中安装了个人防火墙，那么当木马进入计算机时，防火墙可以起到有效的保护作用。

4. 安装系统补丁

用户应该经常安装系统补丁，这样可以减少因系统漏洞带来的安全隐患。

5. 加强个人网络安全保护意识

不要执行来历不明的软件和程序。木马的服务端程序只有在被执行后才会生效。通过网络下载的文件，QQ 或 MSN 传输的文件，以及从他人那复制的文件，对电子邮件附件在没有十足把握的情况下，千万不能将它打开。最好在运行这些软件和程序之前，使用反病毒软件对其进行安全检查。

6. 设置文件扩展名状态

文件扩展名是文件格式和功能的代表，通过文件扩展名，用户一眼就能识别出该文件的真正身份，例如，exe 代表可执行文件，txt 代表文本文件，html 代表网页文件等。知道了文件的扩展名，再查看文件的图标，如果它们之间的对应不一致（如文件扩展名是 exe，但却使用了 txt 的图标）那么就说明这个文件经过了别人的修改，这样的文件大多是木马程序。

但在 Windows 系统中，默认并不显示文件扩展名，因此需要用户修改文件扩展名状态，其修改方法如下：

双击【我的电脑】图标，在打开的【我的电脑】窗口中，单击【工具】菜单，并执行【文件夹选项】命令，如图 3-17 所示。

在【文件夹选项】对话框中切换到【查看】选项卡，在【高级设置】列表中禁用【隐藏已知文件类型的扩展名】复选框，如图 3-18 所示，这样用户可以很容易地查看到文件的扩展名。

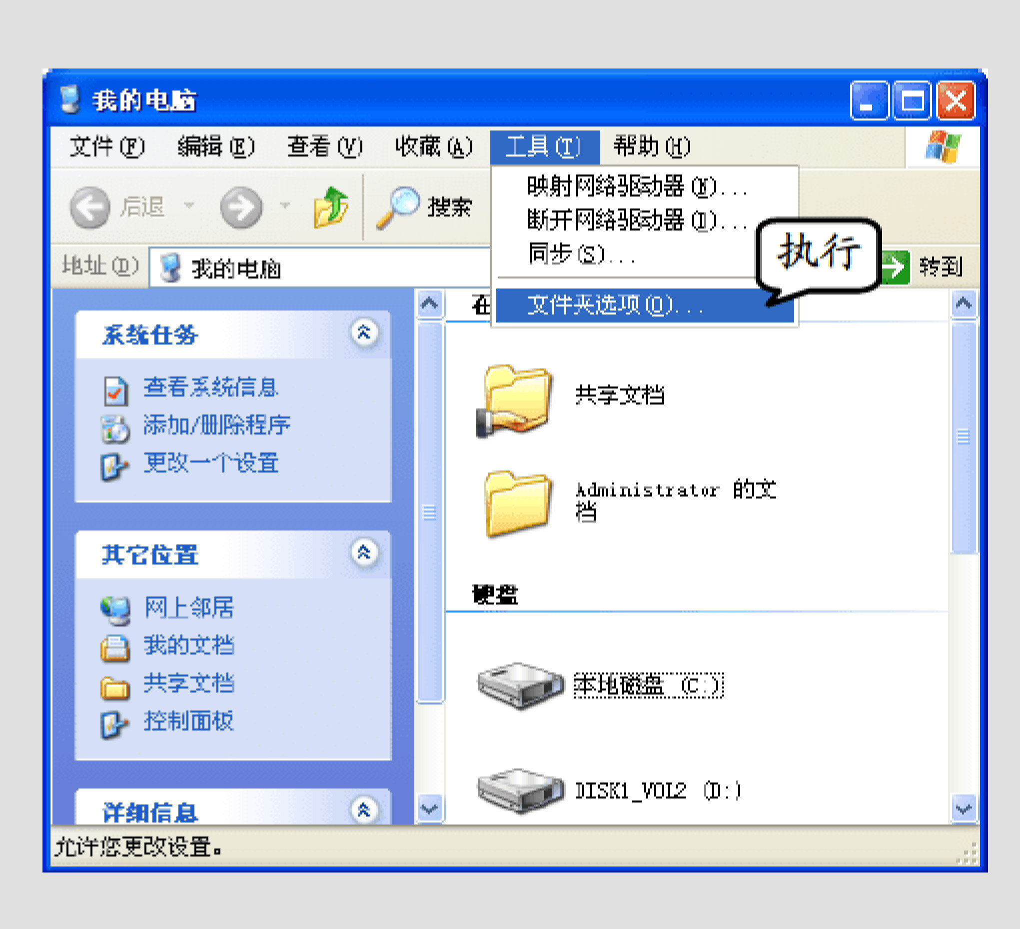


图 3-17 【我的电脑】窗口

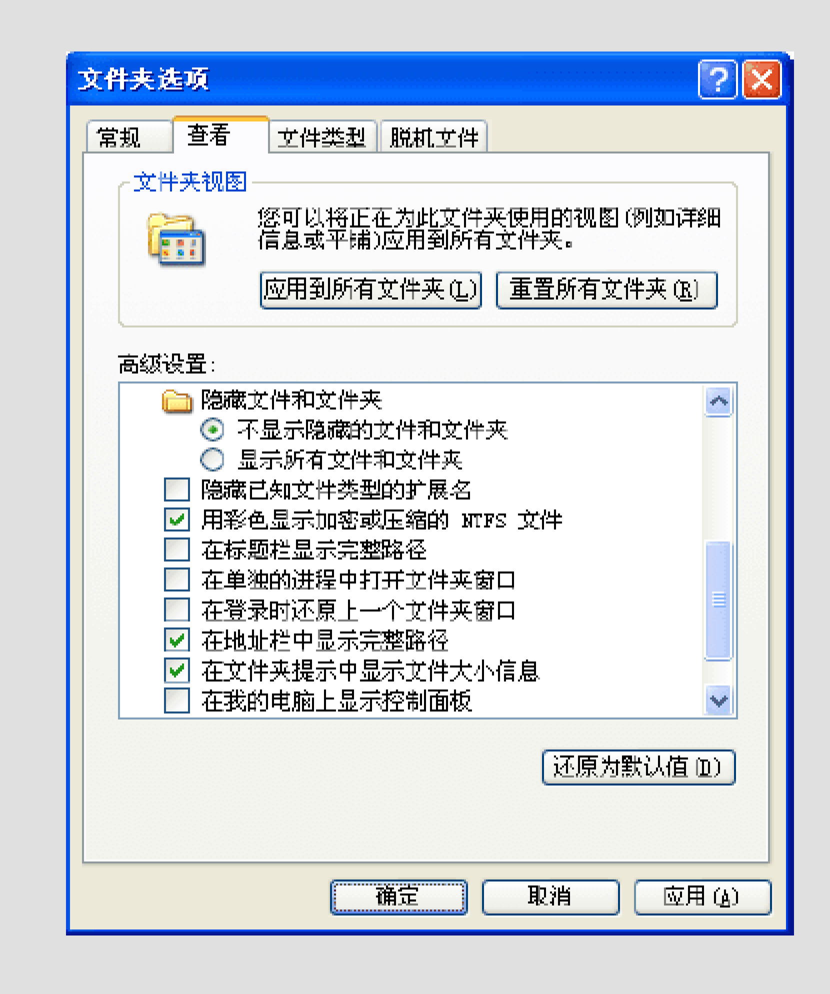


图 3-18 文件夹选项

3.5 操作实例

3.5.1 操作实例——网络信息搜集

网络信息搜集主要表现在撷取网络信息，并尽可能撷取最为详细且重要的网络协议信息。撷取的信息能够帮助用户更清楚地认识网络布局。而通过 Wireshark 这款软件就可以搜集这些网络信息。

1. 实例目的

- 监听网络数据。
- 筛选网络信息。

2. 实例步骤

（1）在桌面右击安装完成后的 Wireshark 应用程序图标，并执行【打开】命令，在软件主界面，单击 Expression 按钮，如图 3-19 所示。



单击 Expression 按钮，可以看到该软件所支持的协议，如 IP、TCP、DNS、SSH 等。

（2）在返回到该软件主界面以后，单击工具栏中的第 1 个按钮，如图 3-20 所示。

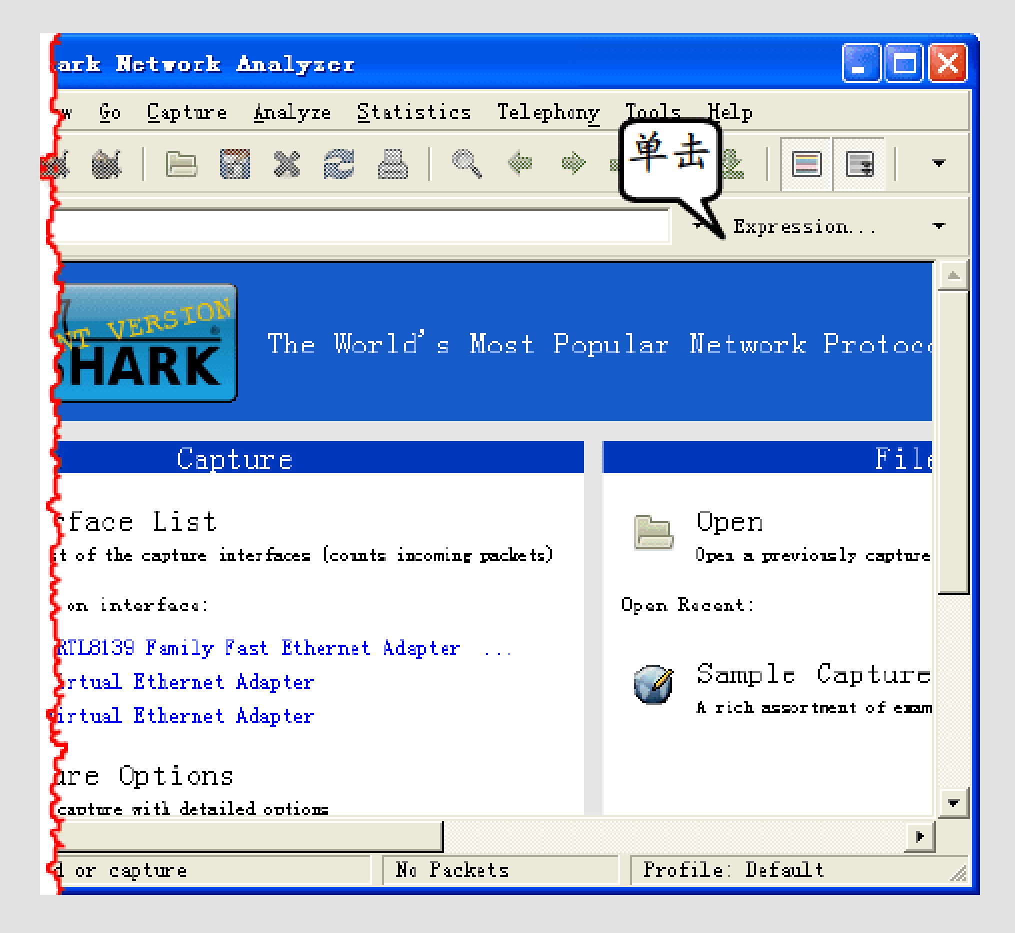


图 3-19 Wireshark 主界面

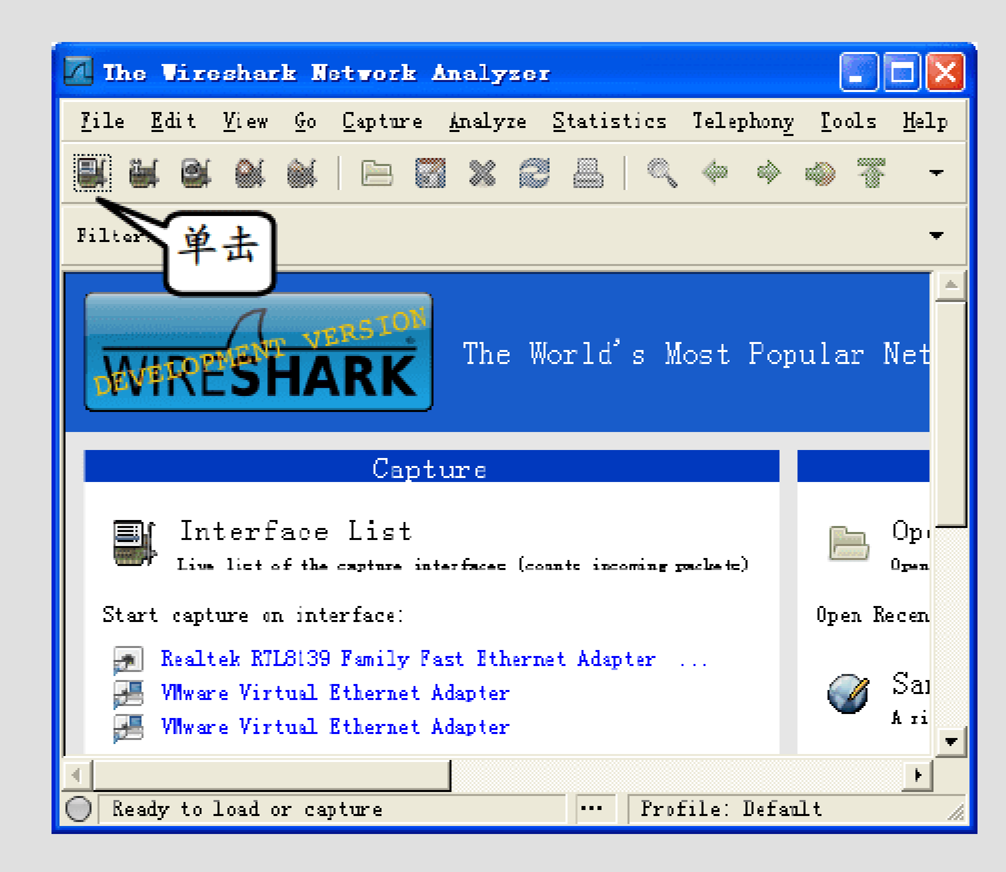


图 3-20 Wrieshark 主界面



最上面的菜单栏中文意思分别是：File（文件），Edit（编辑），View（查看），Go（转到），Capture（捕获），Analyze（分析），Statistics（统计），telephony（手动），tools（工具），Help（帮助）。

（3）在弹出的窗口中，单击 IP 地址 192.168.0.15 这一行的第二个按钮 Options，如图 3-21 所示。

（4）在 Wireshark: Capture Options 窗口中的 Interface 下拉列表框中选择“local”（本地）选项，在“local”后面选择本机使用的网卡，如“Realtek RTL8139 Family Fast Ethernet Adapter”，如图 3-22 所示。

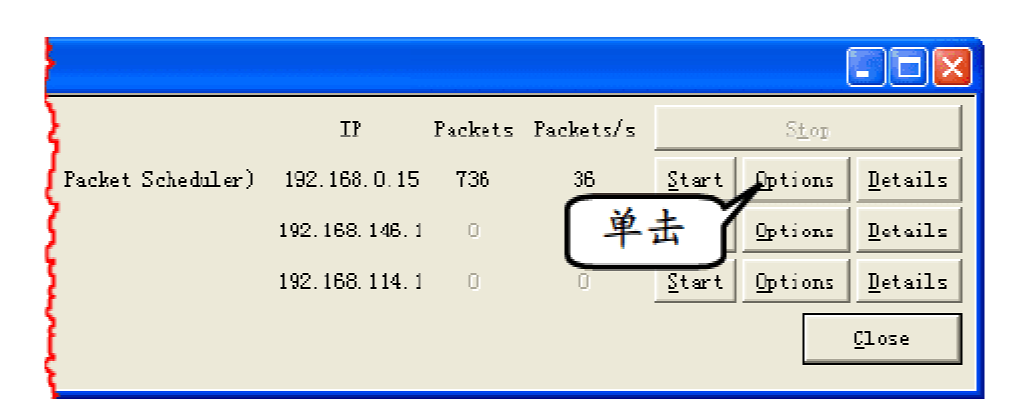


图 3-21　选所要监听的网卡

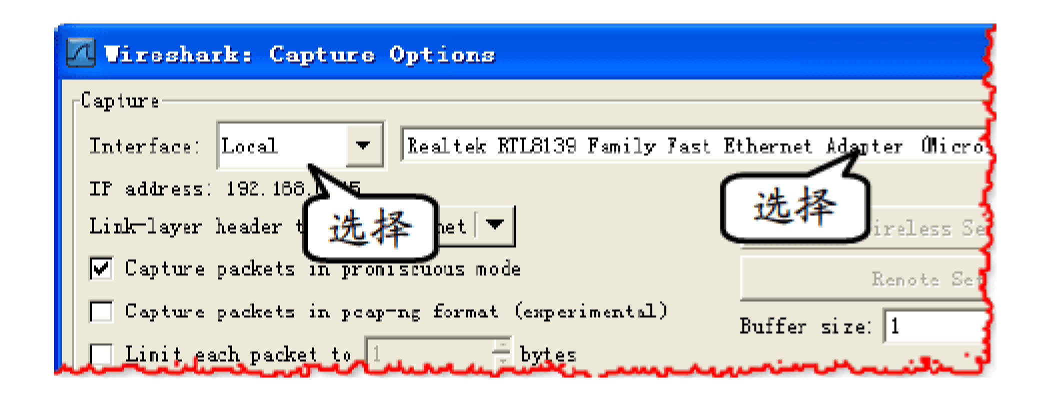
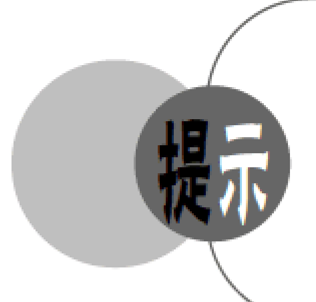


图 3-22　设置本地网卡

（5）在过滤器 Capture Filter 文本框内，输入 ICMP，并单击 Start 按钮，如图 3-23 所示。



在 Capture Filter 文本框内输入 ICMP 是指通过该软件仅抓取 ICMP 包。用户也可以在此输入其他类型的协议名称（如 TCP、UDP 等）以抓取相应的数据包。但在默认未设置情况下，该软件会抓取它所支持协议类型的所有数据包。

（6）在主窗口中，可以查看到该软件当前所捕获的 ICMP 数据包，单击工具栏中的第 4 个按钮（从左至右），并双击该软件所捕获到的第 1 个 ICMP “Request”请求数据包，如图 3-24 所示。

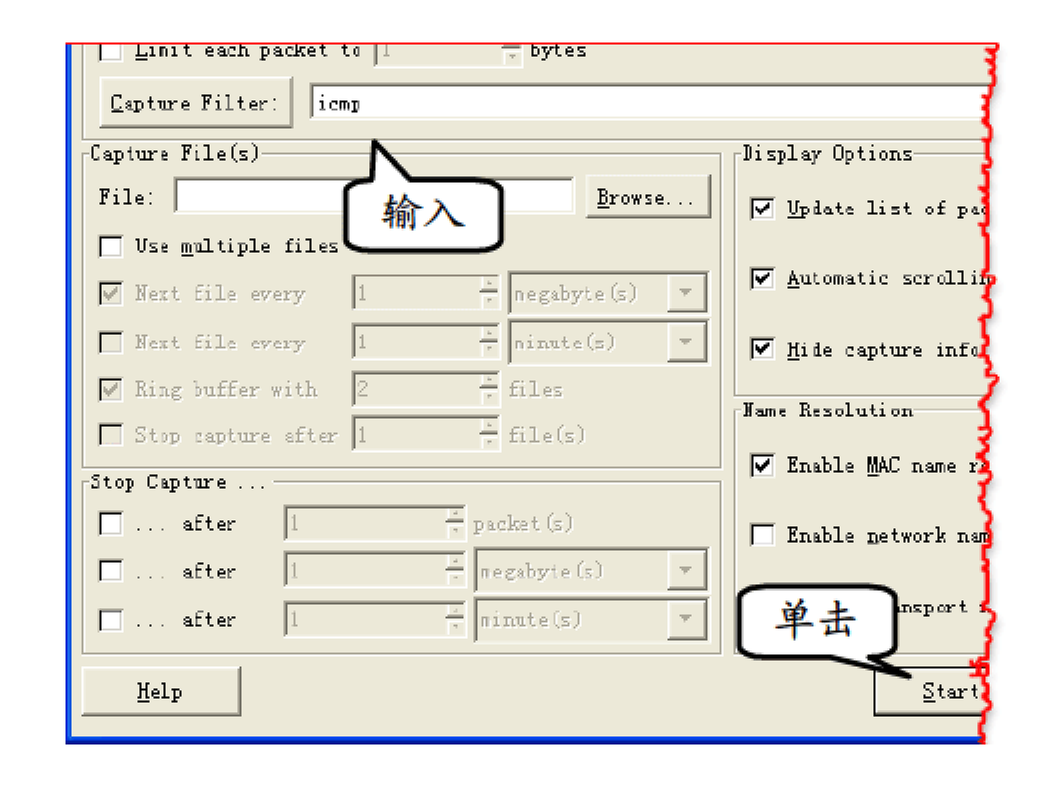


图 3-23　过滤的 ICMP 协议

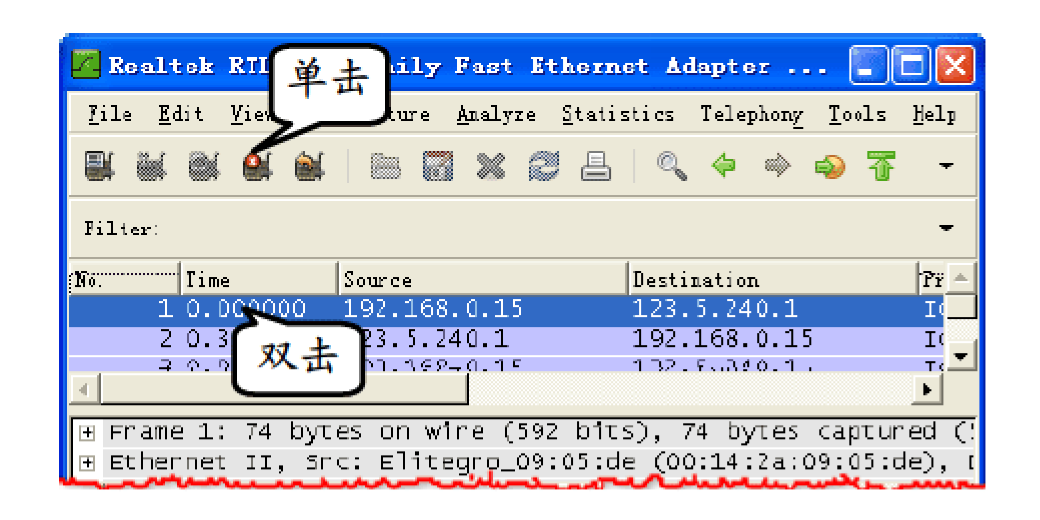
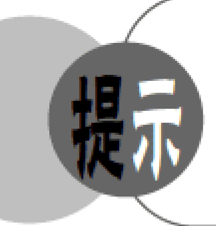


图 3-24　关闭监听并停止抓取数据包



第 4 个按钮的（从左至右）作用是关闭监听，如果用户不关闭监听，那么此软件就会一直进行抓包。

（7）在打开的窗口中，可以查看到该 ICMP “Request”请求数据包的详细内容，如图 3-25 所示。

（8）双击该软件所捕获到的第 2 个 ICMP “Reply”请求数据包，在打开的窗口中，可以

查看到该数据包的详细内容，如图 3-26 所示。

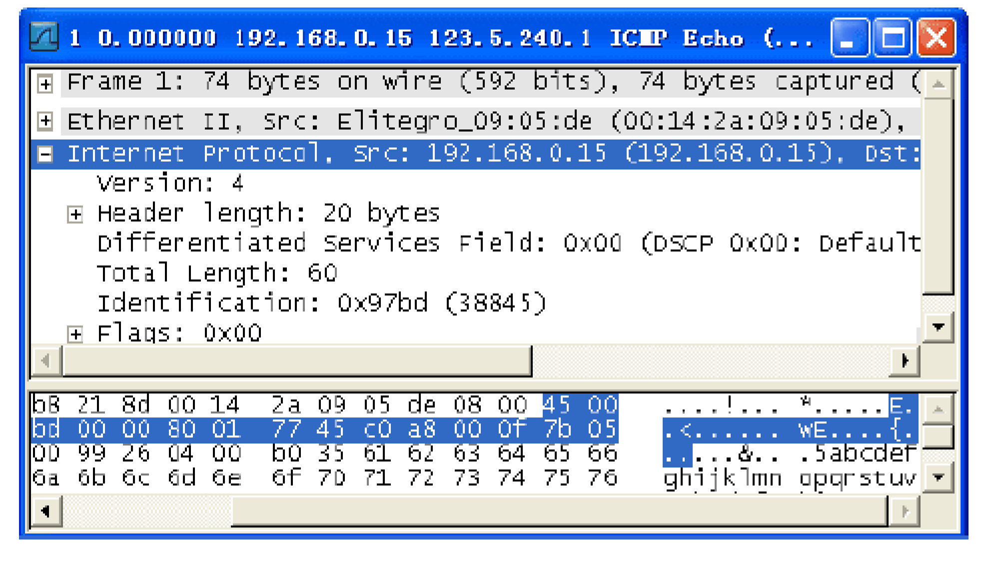


图 3-25　ICMP“Request”请求数据包详细信息

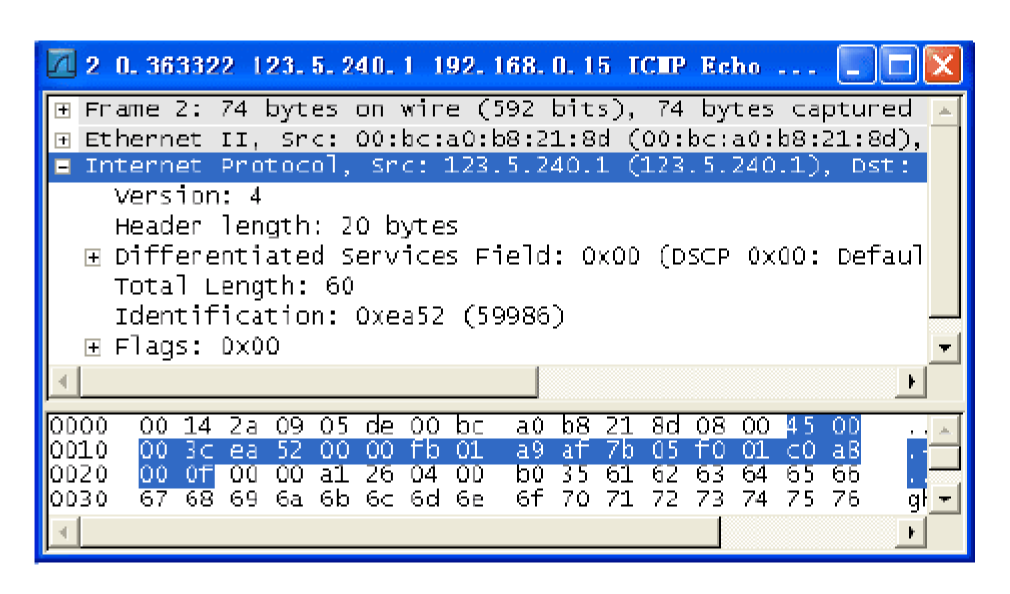
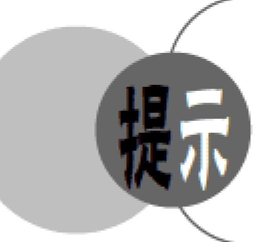


图 3-26　ICMP“Reply”回应数据包详细信息



仔细观察“Request”请求数据包，“Reply”回应数据包，可以清楚地发现 ICMP 报文的格式及相关的网络信息，如源 IP 地址、目标 IP 地址和 MAC 地址。

3.5.2　操作实例——端口扫描

SupeScan 通过 TCP 或 UDP 方式，扫描计算机，探测开放端口，搜集计算机信息，检测安全性弱点。

1. 实例目的

- ❑ 设置扫描选项。
- ❑ 填写扫描参数。
- ❑ 查看扫描结果。

2. 实例步骤

（1）在桌面双击“superscanv4_0_rhc”应用程序图标，如图 3-27 所示。

（2）在 SuperScan 4.0 窗口中，选择【主机和服务扫描设置】选项卡，如图 3-28 所示。



图 3-27　执行程序



图 3-28　SuperScan 4.0 窗口

（3）在【TCP 端口扫描】区域内，选中【直接连接】单选按钮，选择【扫描】选项卡，如图 3-29 所示。

（4）在【扫描】选项卡页面的【主机名/IP】文本框中输入 IP 地址，如“192.168.0.253”，并单击右侧按钮，添加 IP 地址。然后，单击【开始】按钮，如图 3-30 所示。

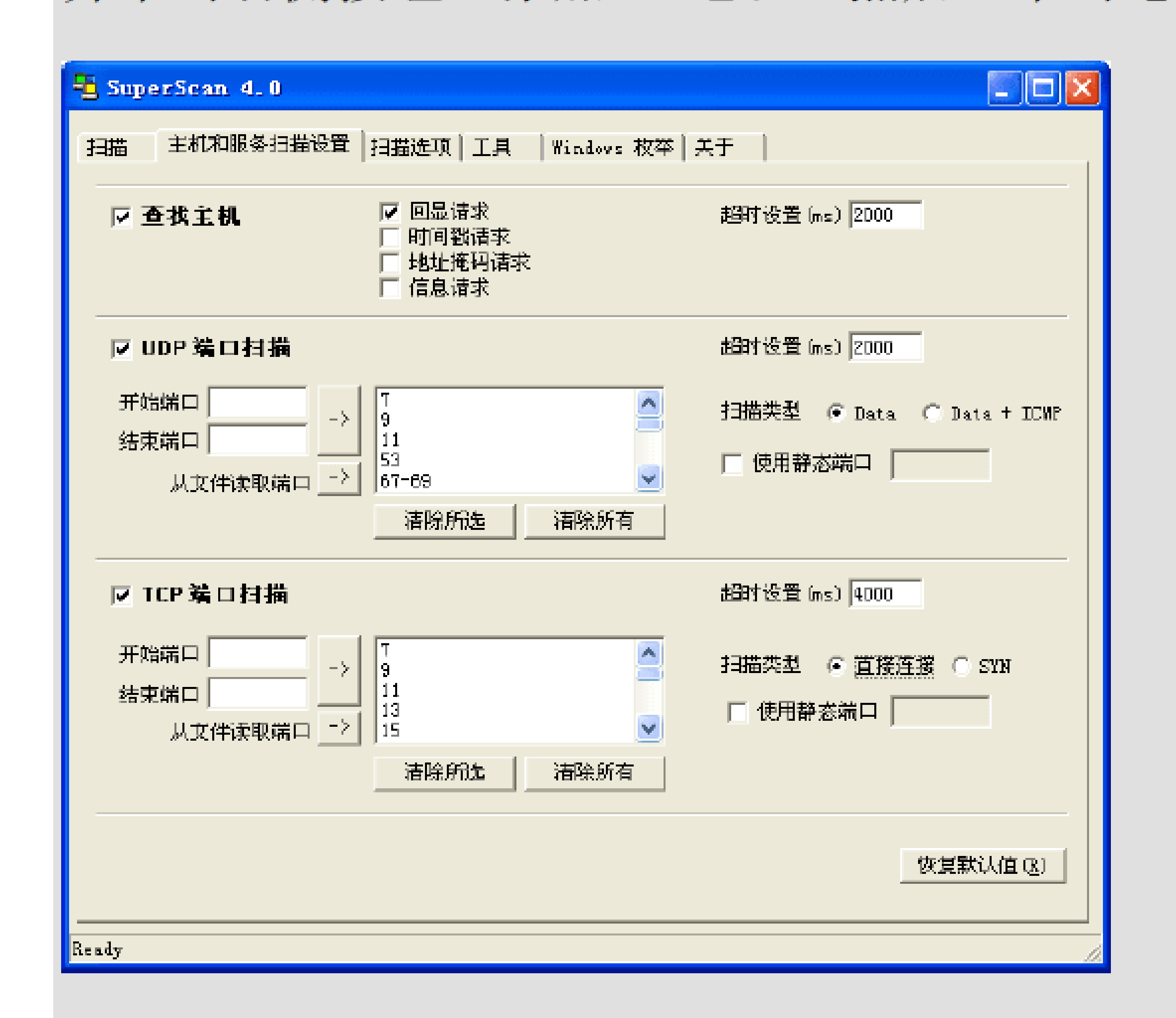


图 3-29　主机和服务扫描设置窗口

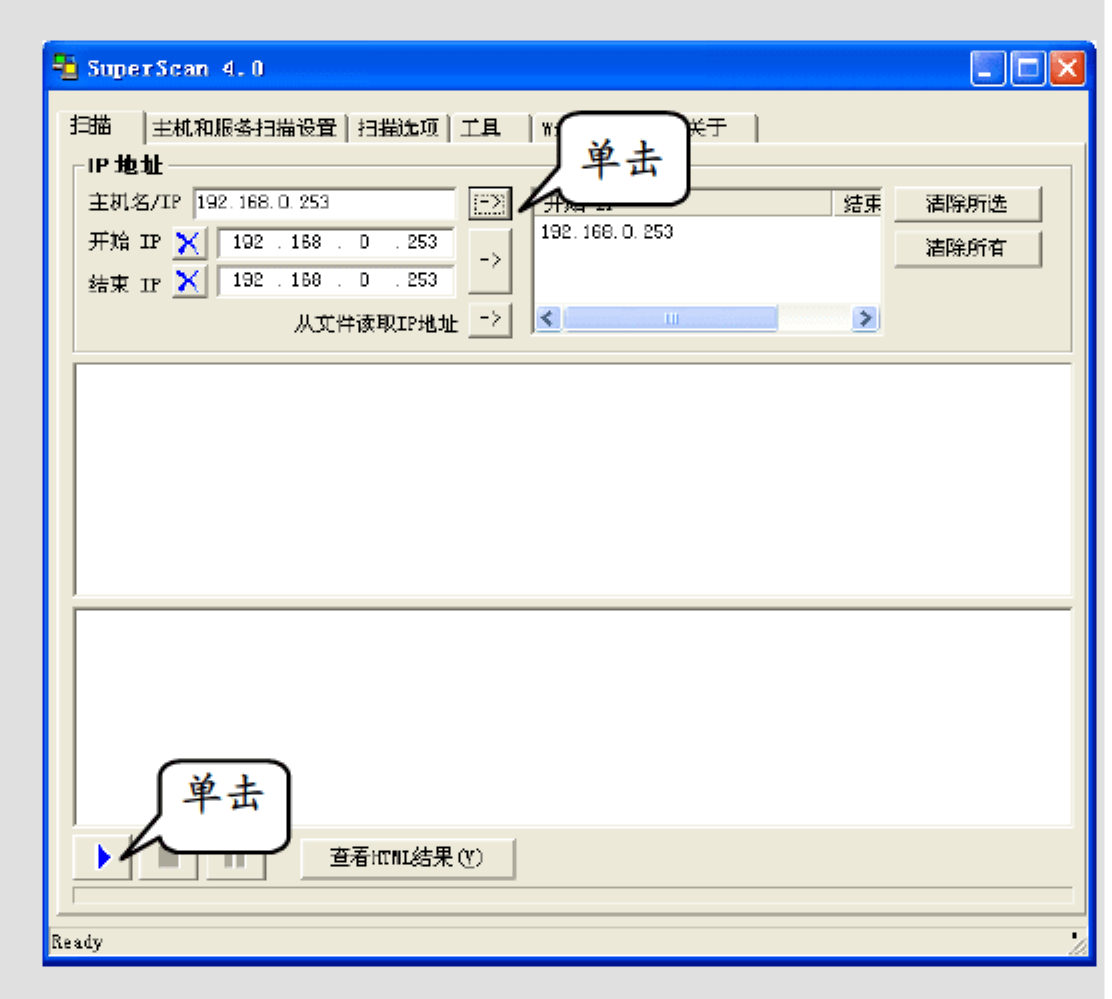


图 3-30　添加扫描地址

（5）扫描完成后，单击【查看 HTML 结果】按钮，即可查看端口扫描结果，如图 3-31 所示。

3.5.3　操作实例——基于认证的入侵防范

随着计算机技术的飞速发展，计算机信息安全问题备受关注。在网络中，通信双方之间建立加密的会话连接能有效防范入侵。这样，即使黑客成功地进行了网络嗅探，但由于捕获的都是密文，因而毫无价值。网络中进行会话加密的手段有很多，可以通过各种认证来防范黑客的入侵，这样就保证信息的安全性。

1. 实例目的

- 捕获网络流量。
- 提取重要安全信息。
- 基于安全信息的入侵。
- 通过认证防范入侵。

2. 实例步骤

（1）在桌面单击【开始】菜单，执行【程序】| Sniffer.Pro | Sniffer 命令，在弹出的对话框中，选择 Realtek RTL8139 Family PCI Fast Ethernet Adapter 选项，并单击【确定】按钮，如图 3-32 所示。



图 3-31　查看扫描结果



图 3-32　【当前设置】对话框



从图 3-32 可以看出计算机所使用的网卡是 Realtek RTL8139 Fast Ethernet Adapter（煜昱快速以太网网卡），因为本计算机装了 Vmware 虚拟机，所以下面的两块是 Vmware 的虚拟网卡。

（2）在该软件主界面中，单击菜单栏中的【监视器】菜单，并执行【定义过滤器】命令，如图 3-33 所示。

（3）在【定义过滤器—监视器】窗口中，选择【地址】选项卡，在【地址类型】下拉列表框中选择 IP 选项，如图 3-34 所示。

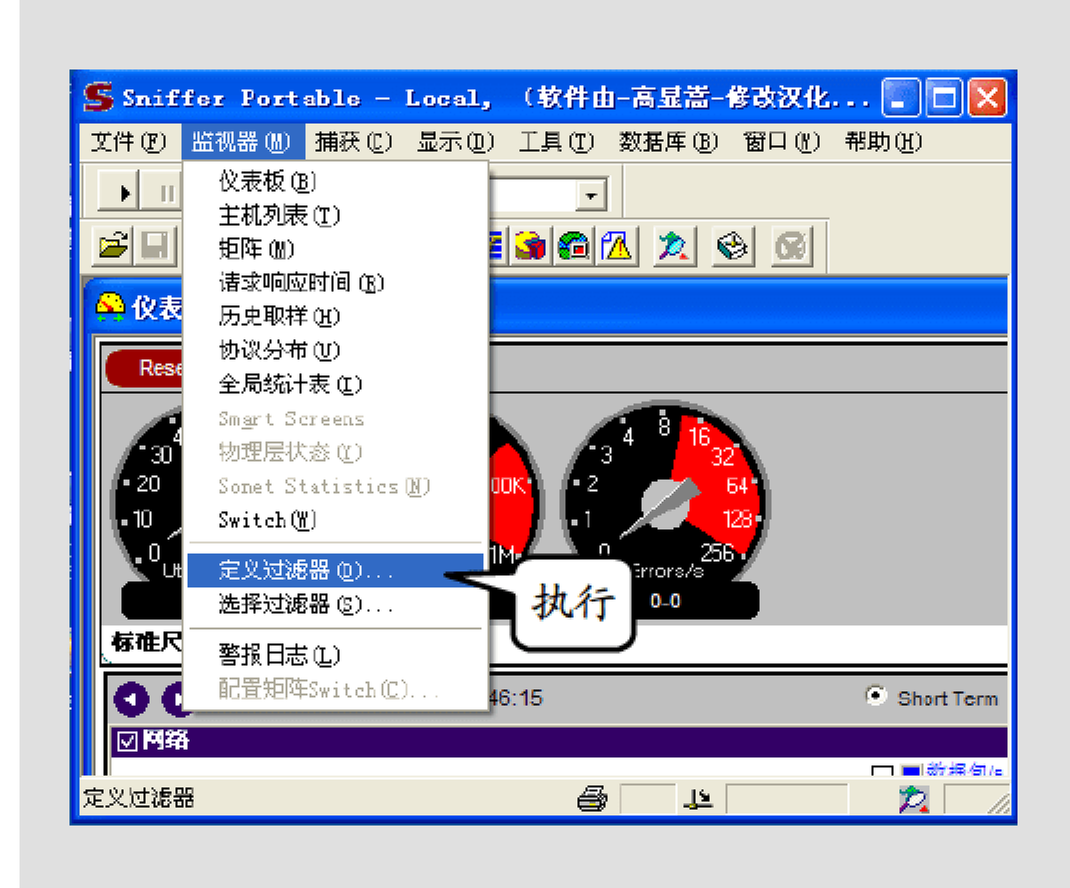


图 3-33　【监视器】菜单

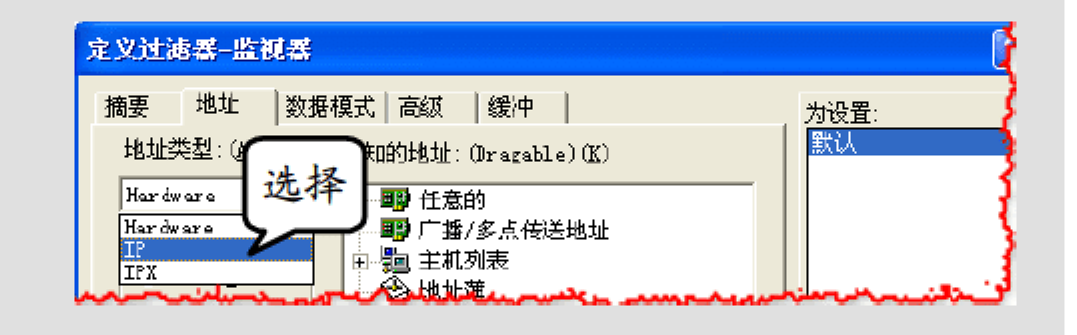


图 3-34　选择 IP 选项

（4）在该对话框中的【位置 1】文本框第 1、2 栏内分别输入 IP 地址 192.168.0.15 和 123.125.50.22，同样在【位置 2】文本框内分别输入 IP 地址，如图 3-35 所示。



过滤源 IP 地址 192.168.0.15 到目的 IP 地址 123.125.50.22 所有数据包。(位置 1 为源 IP 地址，位置 2 为目的 IP 地址，123.125.50.22 是 163 邮箱的 IP。)

（5）在【定义过滤器—监视器】窗口中，选择【高级】选项卡，依次展开【可用到的协议】| ip 节点，并启用 TCP 复选框，之后单击【确定】按钮，如图 3-36 所示。

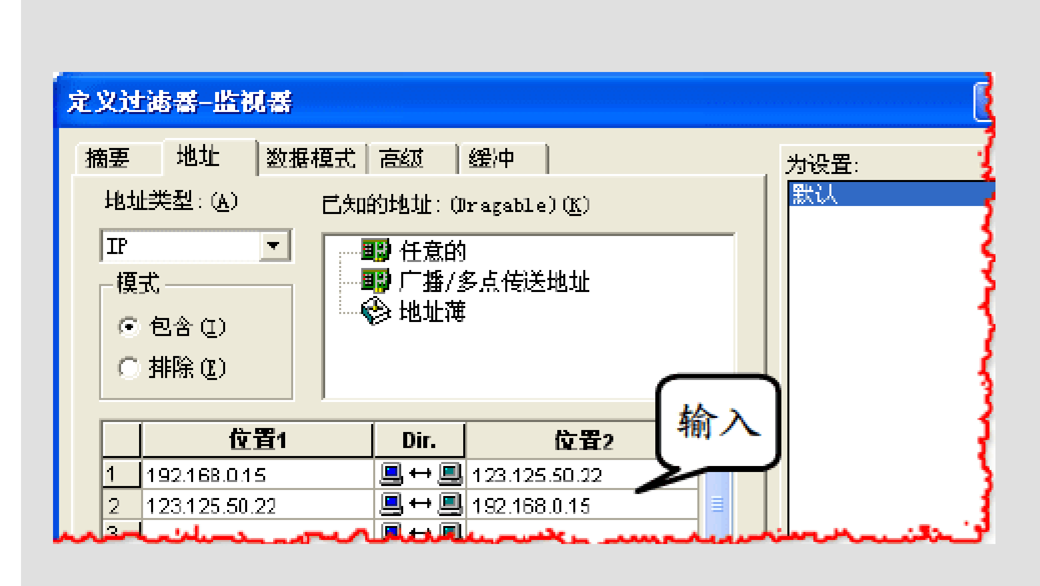


图 3-35　输入要过滤的地址范围



图 3-36　定义过滤器窗口



【高级】选项卡主要是设置需要过滤的协议，选择 TCP 选项的原因是 HTTP(80)和 HTTPS（443）都属于 TCP 协议。

（6）在该软件主界面中，单击【开始】按钮，并打开 IE 浏览器，进入网易 163 邮箱的页面，在【用户名】和【密码】文本框中输入相应信息，单击【登录】按钮，如图 3-37 所示。

（7）在该软件主界面中，单击【关闭并显示】按钮，选择【解码】选项卡，如图 3-38 所示。



图 3-37　输入用户名和密码

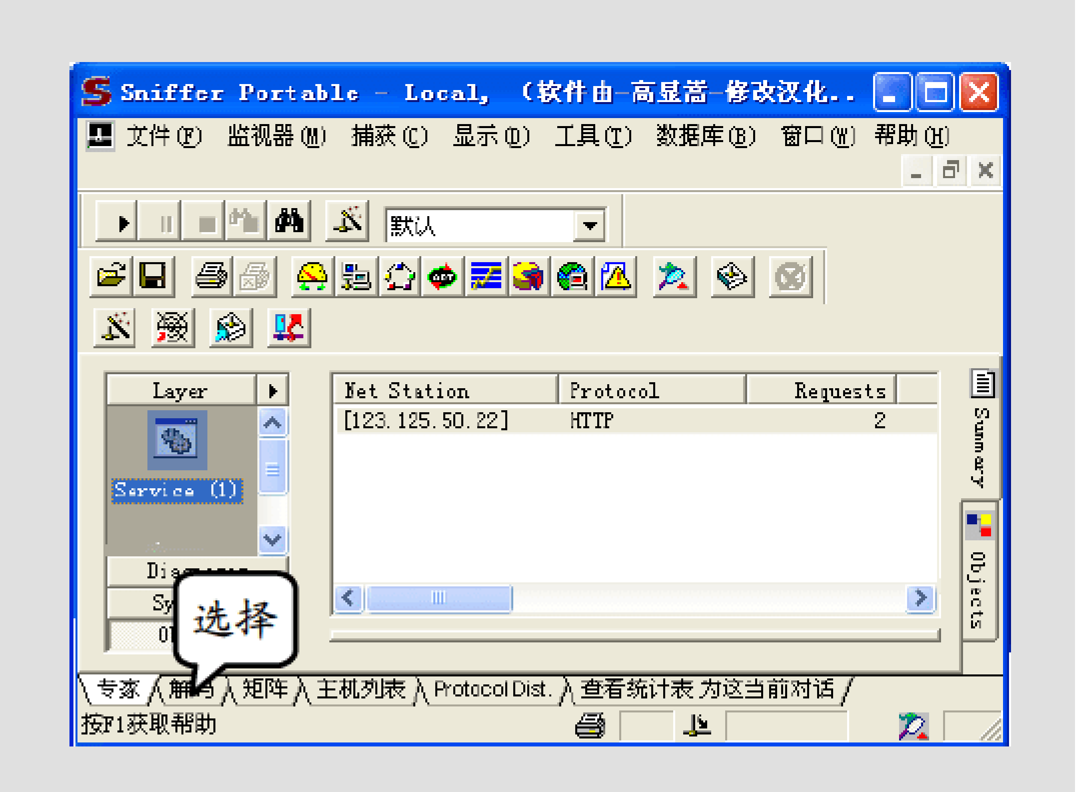


图 3-38　捕获的各层信息



"Layer"下方显示的是各层捕获的信息数量，而在右边的窗格内 IP 是 123.125.50.22，协议是 HTTP，就是所捕获的数据包。

（8）在【解码】选项卡页面中所包含的 HTTP 数据包中，单击含有"POST/login.jsp"字段的数据包，如图 3-39 所示。



使用解码选项来分析 HTTP 数据包，关键是要对各种层次的协议了解得比较透彻，只有这样才能对所截取的数据包进行正确的分析。从解码 HTTP 的数据中能够找出登录的账号和密码等相关信息。

（9）在该软件主界面中，单击【开始】按钮（再次捕获数据包），打开 IE 浏览器，进入 163 邮箱网页，在【用户名】和【密码】文本框中输入相应信息，启用【SSL 安全登录】复选框，并单击【登录】按钮，如图 3-40 所示。

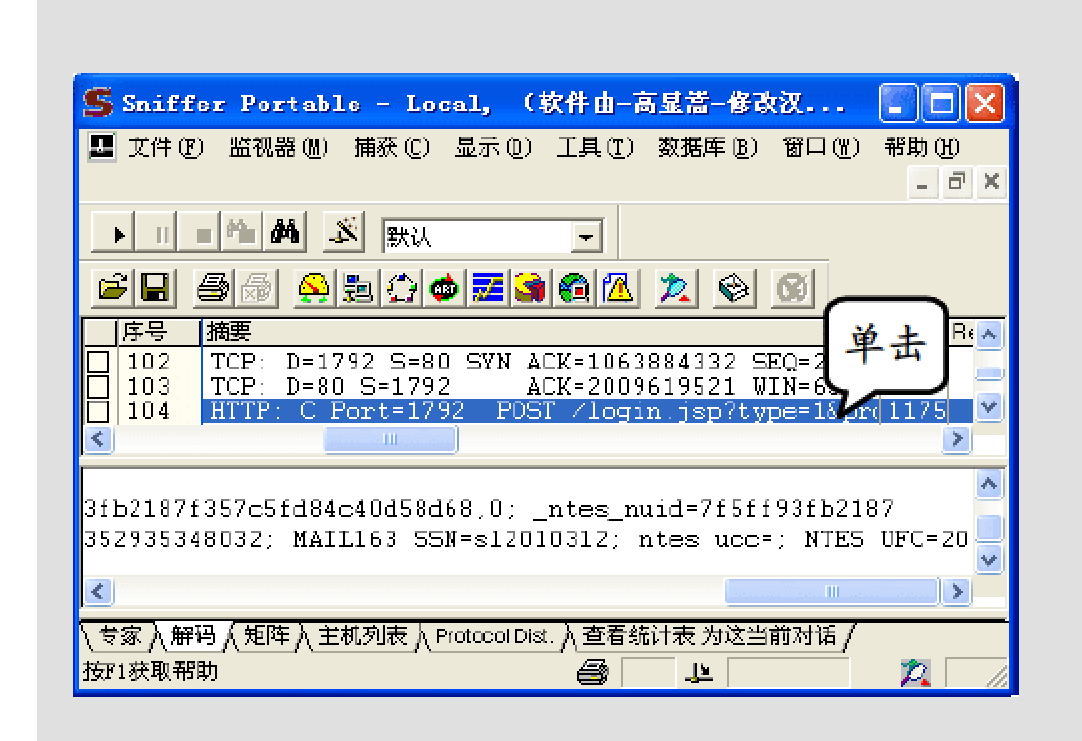


图 3-39　包含 POST 字段的数据包



图 3-40　SSL 安全登录



单击【登录】按钮后，有个页面跳转过程，在页面跳转时能够看见 IE 地址栏中的 http 变成了 https，因为 https 协议调用了 SSL 技术。

（10）在该软件主界面中，单击【关闭并显示】按钮，如图 3-41 所示。

（11）在【解码】选项卡页面中，单击一个 HTTPS 的 TCP 数据包，如图 3-42 所示。



在两次捕获的数据包中，上一次所使用的 http 端口为 80，可以看到这次 https 使用的端口号是 443，使用 SSL 安全登录，从而保证个人信息的安全。

（12）在【解码】选项卡页面所包含的 HTTP 数据包中，单击含有"POST"字段的数据包，如图 3-43 所示。

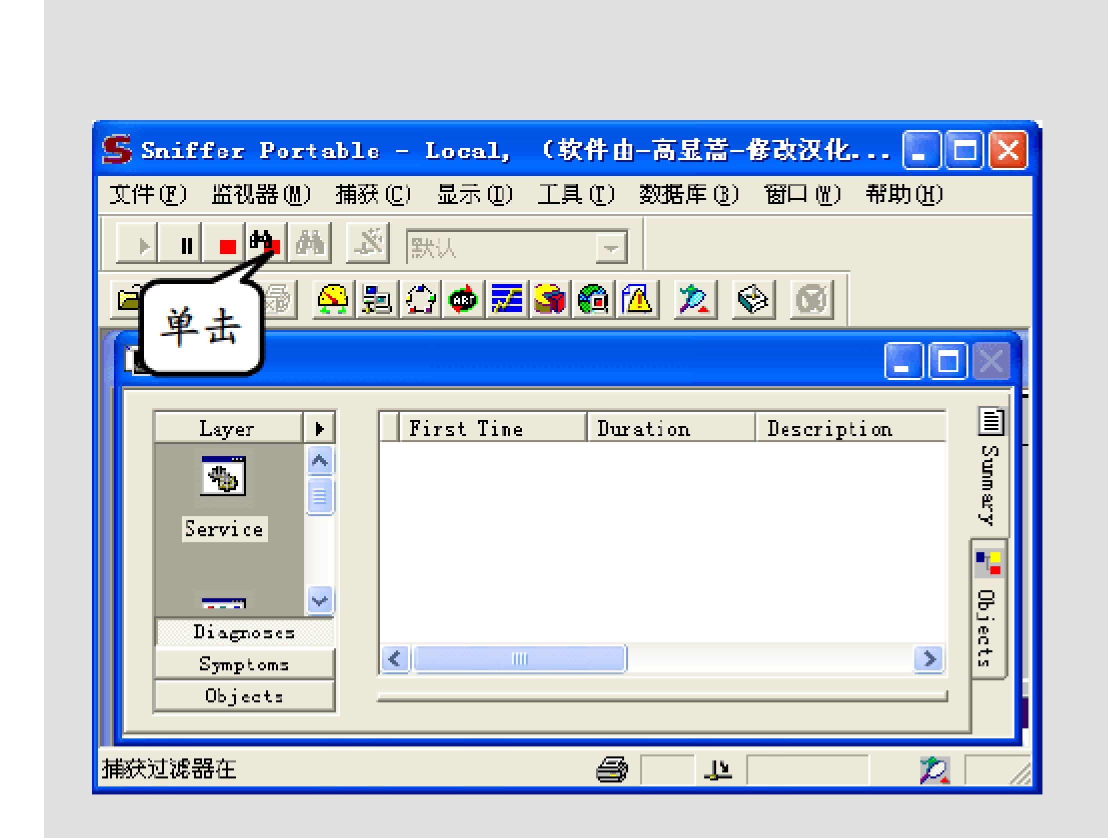


图 3-41　关闭监听，显示数据包

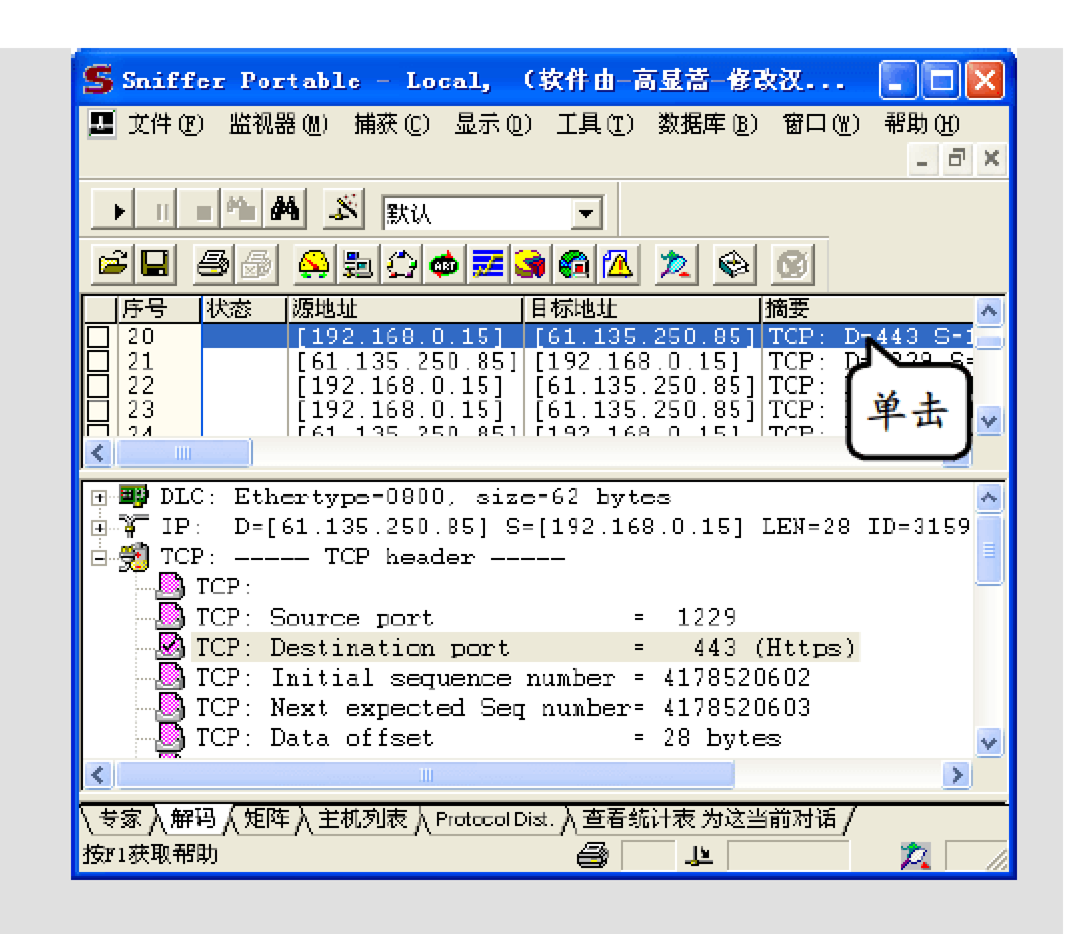


图 3-42　基于认证的数据包

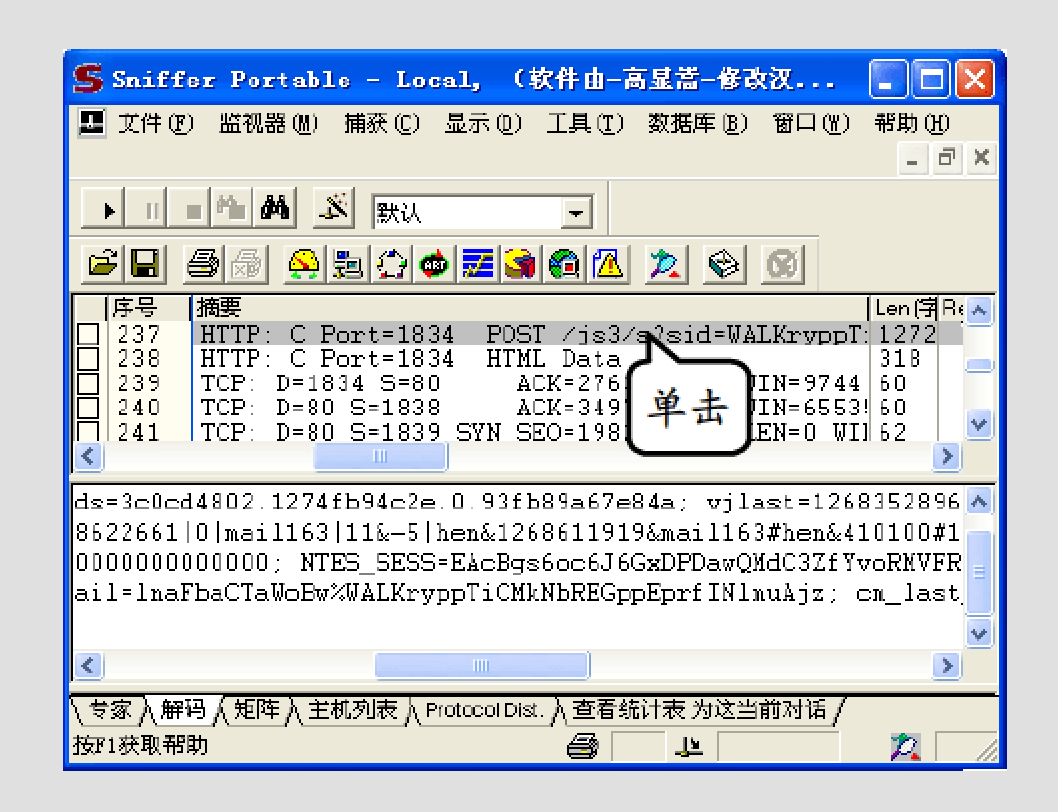


图 3-43　包含 POST 字段的数据



使用 SSL 认证方式，避免了黑客通过嗅探工具截取用户的账号和密码等重要的安全信息。

第二篇　网络操作系统安全

第4章 操作系统加固

目前，Windows Server 2008 是最新的服务器操作系统，具有高性能、高可靠性和高安全性等特点。在默认状态下，Windows Server 2008 在安装完成后已经实施了很多安全策略，但由于服务器操作系统的特殊性，除默认安全策略外，还需要管理员对操作系统进行加固，以进一步提高服务器操作系统的安全性，从而保证业务应用系统和数据库系统的安全性。

本章从操作系统的安装与更新开始来介绍如何正确安装和配置 Windows Server 2008 服务器操作系统。

本章学习要点：

- 了解操作系统及补丁的安装注意事项
- 熟悉系统服务安全中的服务账户
- 了解 Windows 防火墙
- 掌握安全配置向导使用方法
- 熟悉默认共享
- 掌握系统服务配置注意事项

4.1 操作系统安装与更新

为了保证操作系统能够顺利安装，不仅要在安装前作好准备（包括备份文件等），而且为了系统的安全也要采取安全的安装方式。

另外，为了保护 Windows 系统的安全，微软公司会不定期地发布各种更新程序以修补系统漏洞，提高系统性能。因此，系统更新是 Windows 系统必不可少的功能。在 Windows Server 2008 服务器中，为了避免系统漏洞带来安全隐患，必须启用自动更新功能并及时安装补丁。

4.1.1 安装注意事项

为了保证 Windows Server 2008 能够顺利安装，在开始安装前必须作好准备工作，包括检查日志正误、备份文件、断开网络以及断开不必要的硬件连接等。

1. 切断与硬件设备的连接

如果计算机正与打印机、扫描仪或者不间断电源（UPS）等不必要的外部设备相连接，那么应在运行安装程序之前将其断开，以避免安装程序在自动检测这类设备时出现问题。

2．断开网络连接

在网络中可能会有病毒在传播，如果不是通过网络安装操作系统，在安装之前就应断开网络连接或直接拔下网线，以免新安装的系统也被病毒污染。

3．检查系统日志，寻找错误

如果在计算机中，已经安装了其他操作系统，建议使用“事件查看器”查看系统日志，找出可能在升级期间引发的问题的最新错误或重复发生的错误。

4．备份数据

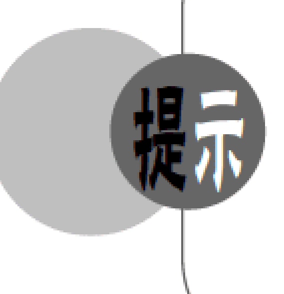
如果服务器中已经安装有其他系统，那么为了避免重要数据丢失，建议在升级前备份有用数据，包括计算机运行所需的全部数据和配置信息，以及所有的用户和相关数据，尤其是那些提供网络服务的数据（如 DHCP 数据）等。建议将文件备份到各种不同的媒介中，例如，磁带驱动器或网络上其他计算机的硬盘，尽量不要保存在本地计算机的磁盘中。

5．检查硬件和软件兼容性

如果要将 Windows 2000 Server 或 Windows Server 2003 升级到 Windows Server 2008，为了保证应用程序的兼容性，可以使用 Microsoft 应用程序兼容性工具包进行检测，以及用来准备安装 Windows Server 2008。

6．加载驱动程序

由于服务器中安装有 RAID 卡等设备，而这些设备可能无法被 Windows 系统所识别，因此，必须在安装之前就加载相应的驱动程序。大多数品牌服务器在出厂时就已经配备了引导光盘，用来加载各种驱动程序并引导安装 Windows Server 2008。因此，建议使用引导光盘安装，如果没有引导光盘，那么安装操作系统之前可以加载 RAID 控制器的驱动程序，否则，无法安装操作系统。至于其他设备的驱动程序，可以在系统安装完成后再安装。



RAID 是英文 Redundant Array of Independent Disks 的缩写，即独立磁盘冗余阵列，或简称磁盘阵列。简单地说，RAID 就是一种把多块独立的硬盘（物理硬盘）按不同方式组合起来形成一个硬盘组（逻辑硬盘），从而提供比单个硬盘更高的存储性能和提供数据冗余的技术。而 RAID 卡就是一种用来实现 RAID 功能的板卡。

7．使用 DVD 光驱

由于 Windows Server 2008 安装程序比较大，安装光盘采用的是 DVD 格式，因此，服务器必须配置 DVD 光驱，而 VCD 则无法读取光盘内容。

另外，在安装 Windows Server 2008 操作系统时，为提高系统安全，建议采用最小化方式安装，只安装网络服务所必需的角色。当产生新的服务需求时，再安装相应的角色，并及时

进行安全设置。

通常，为保证系统初始化安装时的安全，应注意以下事项。

- 确保操作系统来源的合法性。
- 保证硬件设备的可靠性。建议操作系统运行于 RAID 5 方式的磁盘阵列中，确保服务器硬件环境的稳定。
- 将操作系统安装在一个干净的系统分区中。在安装之前，确定磁盘中所有的数据都已经删除干净，磁盘完好无损，最好将涉及的磁盘全部都格式化。合理安排系统安装分区，如 C 盘安装操作系统、D 盘安装数据库系统、E 盘存储日志文件等。
- 在操作系统安装完成后但没有正式运行前，保证系统在安装的过程中不与任何公共的系统相连，如果必须相连，要确保服务器在一个独立可信并且是绝对安全的网段中。
- 不要在服务器上安装多系统启动环境。防止系统因为交叉启动控制而造成引导区或者引导文件的丢失和损坏。
- 如有可能，尽量安装英文版本的操作系统。因为微软公司总是最先发布英文版本的补丁，中文版本的补丁相对滞后一段时间。
- 使用 NTFS 分区作为唯一的文件系统分区标准。NTFS 是真正的日志性文件系统，使用日志和检查点信息，即使在发生系统崩溃或者电源故障的时候也能保证文件系统的一致性。只有使用 NTFS 格式的分区才能对文件使用控制访问列表（ACL）的访问进行控制，达到访问控制安全的目的。
- 仅安装 TCP/IP 协议，如果没有必要不要安装任何其他协议。
- 在安装的过程中，为系统管理员设置一个足够强的复杂密码，长度最好在 20 位以上。

4.1.2　补丁安装注意事项

Windows 系统补丁程序是由微软网站发布的用于弥补相应操作系统漏洞或缺陷的应用程序包。通常有手动安装和自动安装两种方式。手动安装补丁程序多用于不支持自动下载和安装更新内容的 Windows 操作系统（如 Windows 98），或者不方便在线获取更新内容的安装。手动安装补丁程序与普通应用程序的安装比较相似。补丁程序可以通过登录相关网站直接下载，也可以通过购买含有补丁程序的安装光盘获得。

安装最新的服务包补丁程序，可用来修补系统漏洞，避免或减小受到病毒和木马攻击的可能性。

用户可以通过多种渠道获得漏洞补丁程序，但是需要注意的是，这些补丁通常都是针对特定产品的，安装之前必须仔细阅读相关文档，这包括如下 3 个方面内容。

1. 阅读补丁声明

在运行补丁程序之前，一定要仔细阅读有关的说明文档，充分了解补丁的功能、用法、对应漏洞的情况，对安装补丁后发生的后果要做到心中有数。然后根据企业的网络环境进行分析，判断可能产生的安全风险，根据漏洞的紧急情况，判断是否需要安装补丁。需要提前做好预备工作，确保针对在补丁安装完成后出现的问题，能有高效、快捷、安全的补救措施。

2. 正确下载补丁

注意补丁程序对应的操作系统和应用软件的版本。很多补丁都是针对某个特定的操作系统和应用软件版本而开发的。另外，在使用时还要下载与操作系统（不同语言版本）应用程序相匹配的补丁程序。

3. 下载安全补丁

补丁的来源一定要安全，必须在可靠的平台下载，或者到由安全认证的供应商那获取相关的补丁程序，防止被恶意修改或安装了嵌入有“木马”程序的补丁。建议到官方网站或信誉度较好的网站下载补丁安装或者在线安装补丁，这样，一方面可以保证下载的补丁是安全有效的，另一方面可以保证补丁安装包的时效性。

除以上 3 点需要特别注意外，在安装系统补丁的时候还应该注意以下问题。

❑ **断开网络连接**

计算机在没有安装补丁之前一定要断网。所需的补丁程序在其他计算机上下载后，使用移动存储设备或者刻录成光盘，复制到需要安装补丁的服务器，再进行安装。

❑ **安装顺序**

某些补丁程序对安装顺序有要求，例如，Windows Server 2003 的某些系统补丁程序就要求必须先安装 Windows Installer 3.0，否则其他补丁安装无法完成。

❑ **安装目录**

安装过程中如需确认或更改安装目录的，建议保持系统默认设置。

❑ **关闭非必需应用程序**

在开始安装补丁程序前应首先关闭其他应用程序，以免导致安装失败。另外，有些补丁程序安装完成后需要重新启动计算机方可生效，应注意及时保存当前打开应用程序的结果。

❑ **版本要求**

获取补丁程序时应注意其版本要求，不仅要注意 Windows 操作系统的类型，还应注意英文版和简体中文版、繁体中文版之间的区别。

❑ **Service Pack 包**

对于 Service Pack 包，应从可信的渠道获得微软的服务安装程序的 Service Pack 包，例如，从微软的官方站点下载。

❑ **HotFix**

微软提供了 Windows Update 程序，可以直接连接到微软的安全更新网站，获取最近更新的 HotFix（即服务包发布之后的安全补丁程序，通常用来弥补最新出现的安全漏洞）。

❑ **Microsoft Update 网站**

微软还提供了一个安全更新网站——Microsoft Update，它可以帮助用户更新 Microsoft Windows 以及安装的许多其他 Microsoft 程序，例如 Microsoft Office、Microsoft Exchange Server 和 Microsoft SQL Server 等，所有更新程序都可以很方便地获得。

❑ **重新启动系统**

在 Windows 中安装 Service Pack 或者 HotFix 时，经常需要重新启动服务器。建议根据系统提示进行系统重启，不要因为怕麻烦而减少系统启动的步骤，否则，可能会造成一些意想不到的故障。

4.1.3　补丁安装

Windows 操作系统补丁的安装方法有多种，下面以 Microsoft Windows Update 联机更新补丁的方式来介绍如何自动更新补丁。

在 Windows Server 2008 中，执行【开始】|【所有程序】|Windows Update 命令，打开 Windows Update 窗口。如果是首次运行 Windows Update，那么系统将检查当前的操作系统中是否已经启动自动更新，检查完成后将提示网络管理员启用 Windows Update，此时单击【立即启用】按钮即可，如图 4-1 所示。

接着，系统将检测更新，由于是重新运行 Windows Update，系统会提示安装新的 Windows Update 软件，此时单击【现在安装】按钮，如图 4-2 所示。

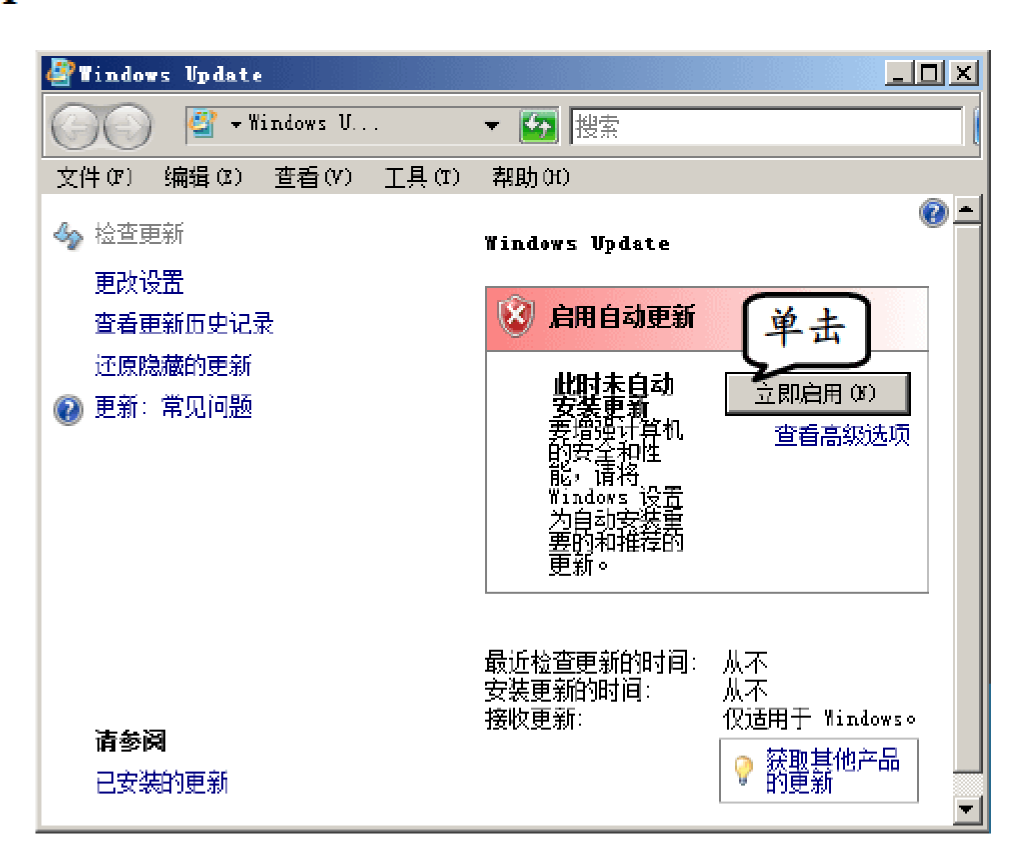


图 4-1　Windows Update 窗口

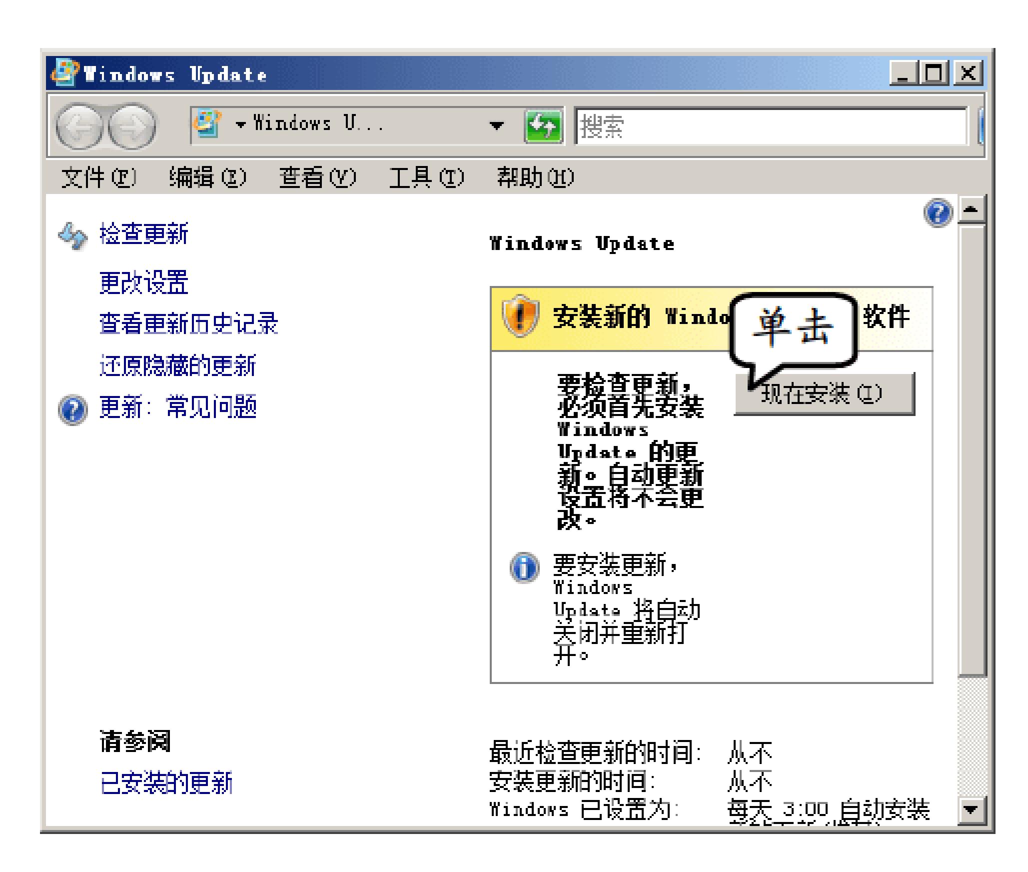


图 4-2　安装新的 Windows Update 软件

当新的 Windows Update 软件更新完成后，该软件将自动关闭并重新打开，此时，单击【检查更新】按钮，如图 4-3 所示。

当可用更新检查完成后，只需单击【安装更新】按钮即可，如图 4-4 所示。在安装时用户需要根据提示同意安装更新。当安装完成后，还需要用户重新启动计算机。

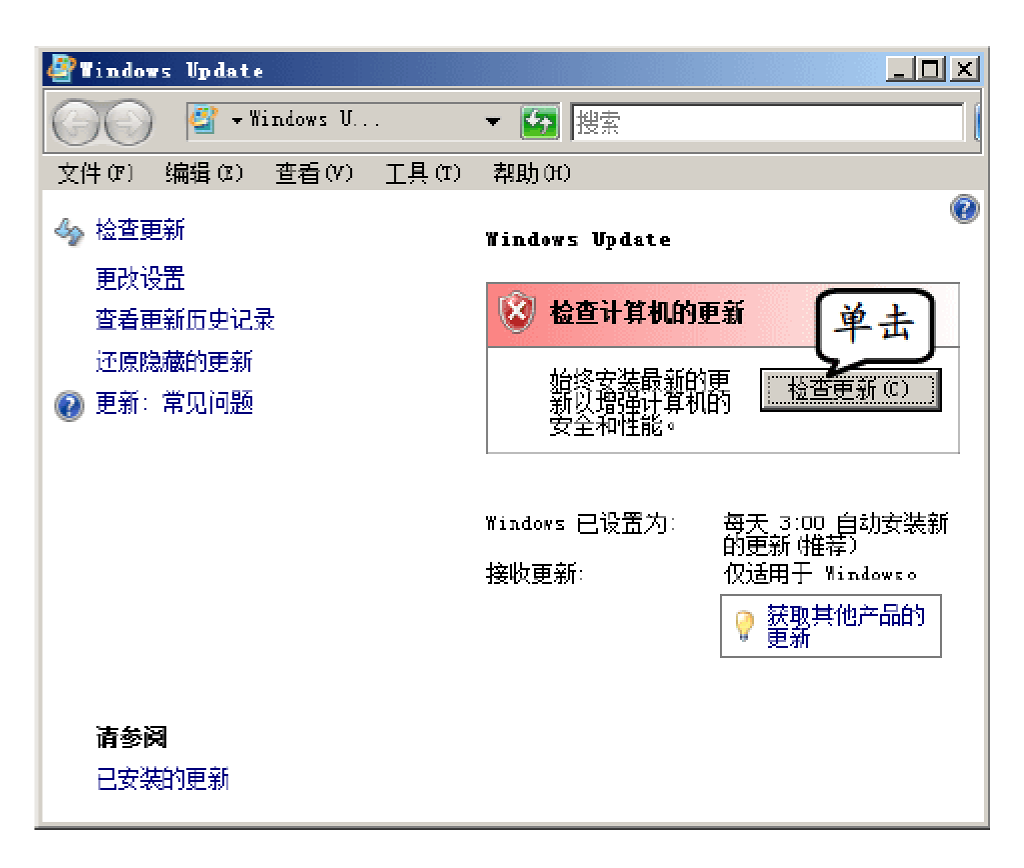


图 4-3　检查更新

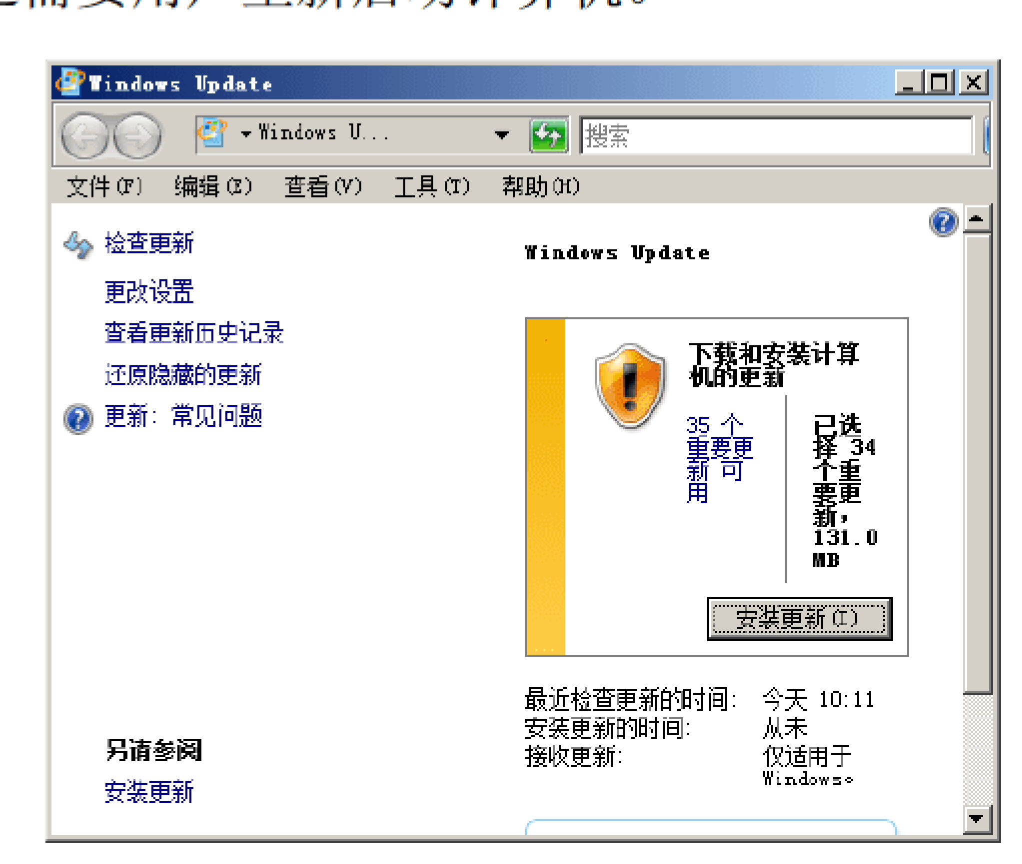
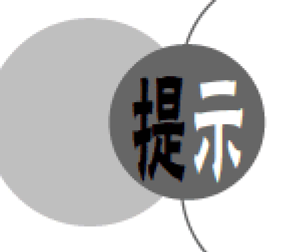


图 4-4　安装更新



系统补丁程序虽然对操作系统有益，但是有些对系统环境要求严格的硬件可能会在安装补丁程序后出现应用故障，必要时可以采取卸载最近安装的补丁程序的方法来排除故障。

当计算机重新启动后，再次打开 Windows Update 窗口，通过选择【查看更新历史记录】选项，可查看补丁安装结果列表，如图 4-5 所示。

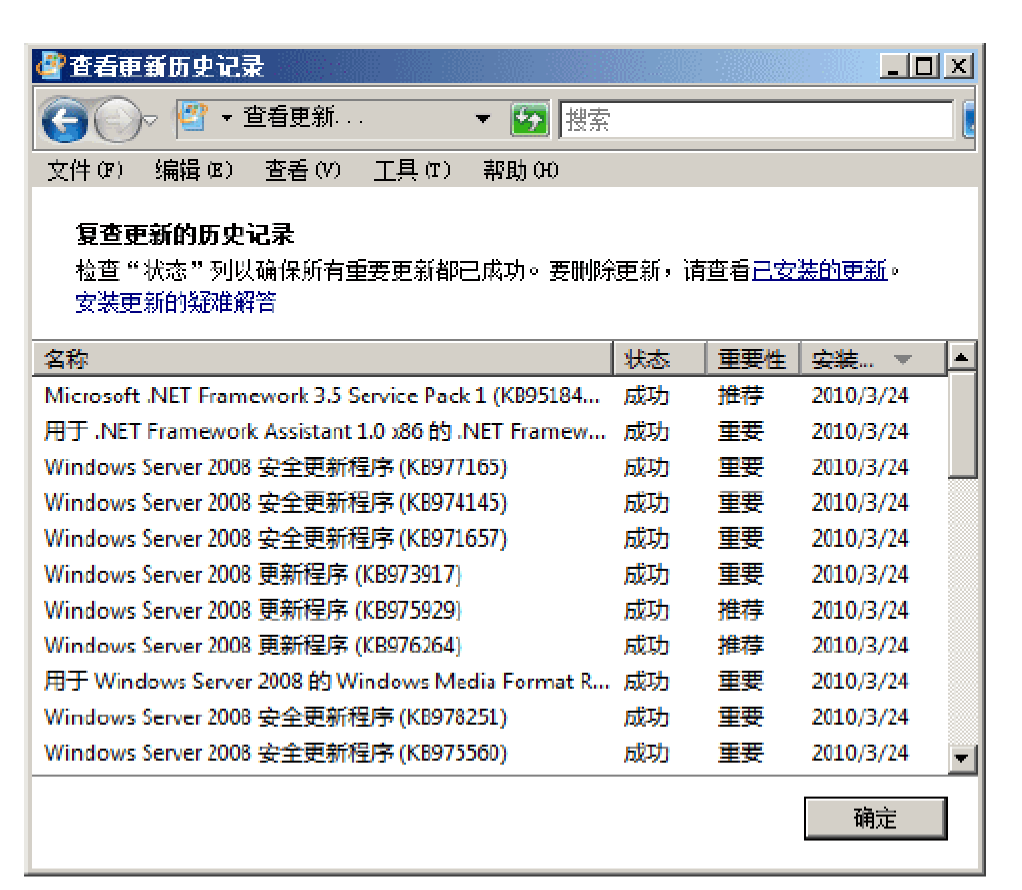


图 4-5　查看安装补丁

4.1.4　网管心得——系统服务安全中的服务账户

服务仅在登录到某一账户的情况下才能访问操作系统中的资源和对象。大多数服务都不会更改默认的登录账户，更改默认账户可能导致服务失败。如果选定账户没有登录计算机服务的权限，Microsoft 管理控制台的服务管理单元将自动为该账户授予登录服务的用户权限，但并不一定会启动服务。

与 Windows Server 2003 相同，在 Windows Server 2008 操作系统中也包括 3 个内置的本地账户，分别用作各系统服务的登录账户。

1. 本地系统账户

本地系统账户的名称是 LocalSystem，没有密码设置，功能强大。它可以对本地系统进行完全访问，并为网络中的计算机提供服务。有些服务的默认配置使用的是本地系统账户，则不需要更改默认服务设置。如果某服务登录到域控制器使用的是本地系统账户，则该服务可访问整个域。

2. 本地服务账户

本地服务账户是一种特殊的内置账户，类似于经过身份验证的用户账户。就访问资源的对象而言，本地服务账户与 Users（用户）组成员具有相同的权限。这种限制性访问有助于在

个别服务或进程受损时保障系统安全，以本地服务账户运行的服务使用有匿名凭据的空会话来访问网络资源。本地服务账户名称为 NTAUTHORITY\LocalService，且该账户没有密码。

3. 网络服务账户

网络服务账户也是一种特殊的内置账户，类似于经过身份验证的用户账户。就访问资源的对象而言，“网络服务”账户与“Users”组成员权限等同。这种限制性访问有助于在个别服务或进程受损时保障系统安全，以“网络服务”账户运行的服务可使用计算机账户的凭据来访问网络资源。账户名称为 NTAUTHORITY\NetworkService，该账户没有密码。



如果更改默认服务设置，那么重要的服务可能无法正常运行。最重要的是，更改启动类型一定要小心谨慎地进行，要使用配置了自动启动服务的设置进行登录。

4.2 Internet 连接防火墙

Windows Server 2008 的防火墙是一款基于主机的状态防火墙，在系统安装完成后就已经被预先安装，与 Windows Server 2003 相比不仅安全性更高，而且更易于管理和配置。

4.2.1 Windows 防火墙简介

默认状态下，Windows 防火墙已经处于开启状态，能够提供基本的安全防护功能，保护内部网络免受恶意攻击者的入侵。除了默认设置外，用户还可以根据需要开启或关闭防火墙。在 Windows Server 2008 中，Windows 防火墙的基本配置变化不大，只要拥有系统管理员权限的用户账户，都可以配置 Windows 防火墙。

在 Windows Server 2008 中，账户控制功能默认是开启的，普通账户必须得到管理员账户的授权后，才可以配置 Windows 防火墙。

执行【开始】|【控制面板】命令，在打开的窗口中双击【Windows 防火墙】图标，即可进入【Windows 防火墙】窗口。在该窗口中，选择【更改设置】选项，可以打开【Windows 防火墙设置】对话框，如图 4-6 所示。

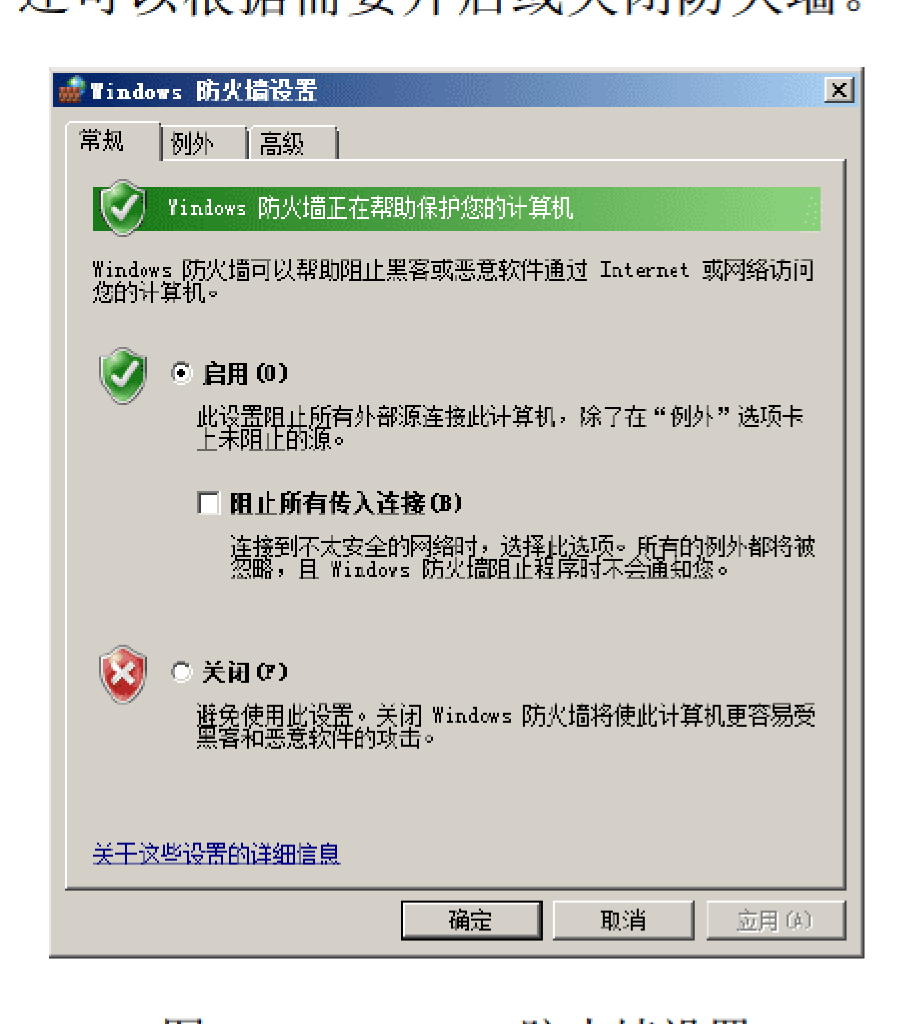


图 4-6　Windows 防火墙设置

1.【常规】选项卡

在【常规】选项卡中，可以为所有连接启用或关闭 Windows 防火墙，而且【阻止所有传入连接】复选框也是一个非常好的选项，特别是当前连接到的网络存在严重的安全隐患时，该选项能够临时让系统禁止【例外】选项卡中设置的任

何程序或服务访问网络，一旦本地服务器系统处于一个比较安全的工作环境时，再禁用【阻止所有传入连接】复选框，恢复之前的正常操作。

启用了服务器系统的防火墙功能后，在默认状态下，该防火墙程序会同时拦截所有程序去访问外部网络，除了在【例外】选项卡中设置的选项外。Windows 防火墙有如下 3 种设置。

❑ **启用**

Windows 防火墙在默认状态下处于打开状态，建议保留此设置。此时，Windows 防火墙会阻止所有到计算机的未经请求的连接，但不包括在【例外】选项卡中选择的程序或服务所发出的请求。

❑ **阻止所有传入连接**

如果启用该复选框，那么 Windows 防火墙会阻止所有到计算机的未经请求的连接，且【例外】选项卡中的程序和服务也将不能连接网络。使用该设置可以为计算机提供最大程度的保护，但此时某些程序也可能会无法正常工作。

❑ **关闭**

如果关闭 Windows 防火墙，那么计算机很容易受到非法入侵者或者 Internet 病毒的侵害。该设置适用于高级用户，或计算机中安装有其他防火墙。

2.【例外】选项卡

在【例外】选项卡中，可以设置能够直接访问网络的程序或服务，可以依次单击【添加程序】按钮、【添加端口】按钮来自行添加需要访问外部网络的程序或服务，从而解除系统防火墙程序对网络访问的阻止，图 4-7 所示为【例外】选项卡。

3.【高级】选项卡

在【高级】选项卡中，可以根据本地服务器系统中多个网络连接的情况，选择需要受防火墙保护的目标网络连接。如果发现防火墙中有许多参数没有配置正确，或防火墙出现故障，用户可以通过单击【还原为默认值】按钮，如图 4-8 所示。这样能够快速取消所有的参数修改操作，将系统防火墙的参数设置恢复到系统初始状态。

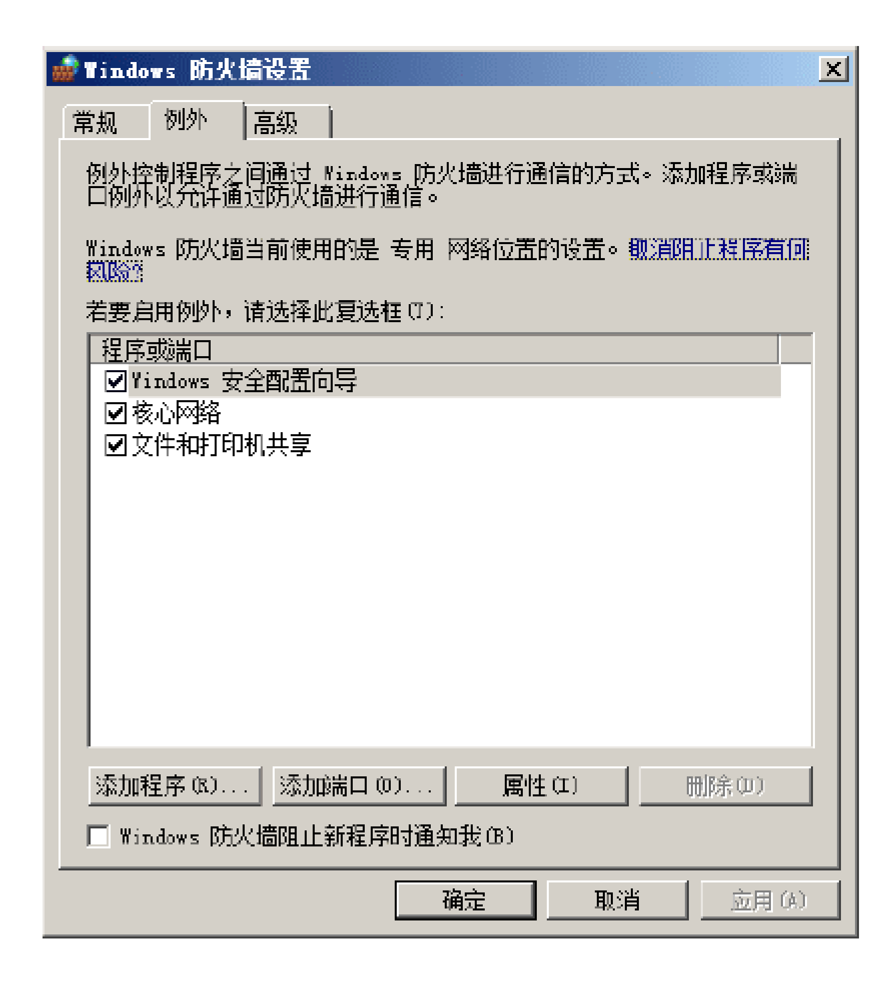


图 4-7 【例外】选项卡

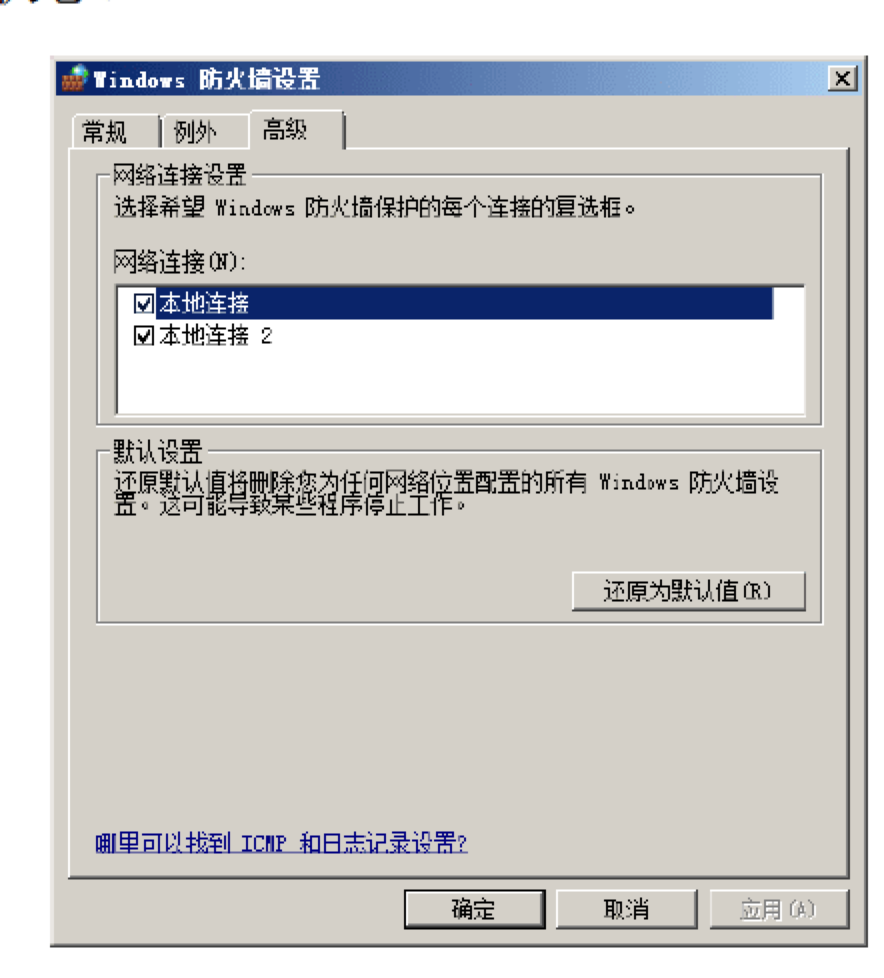


图 4-8 【高级】选项卡



还原为默认值后，用户自定义的所有“例外”项目也都将被删除，所有设置和选项都将还原到原始状态。

4.2.2　启用 Windows 防火墙

Windows Server 2008 自带了 Windows 防火墙功能，可以有效地防止服务器上未经允许的程序与网络进行通信，从而在一定程度上保护了服务器与网络的安全。如果要运行某个程序与网络进行通信，可以将其添加到 Windows 防火墙的“例外”中。

在默认状态下，Windows Server 2008 系统安装完成后，Windows 防火墙为开启状态。用户可以通过执行【开始】|【控制面板】|【Windows 防火墙】命令，打开【Windows 防火墙】窗口，如图 4-9 所示。

在【Windows 防火墙】窗口中，单击【更改设置】链接，在弹出的【Windows 防火墙设置】对话框中，默认选中【启用】单选按钮，如图 4-10 所示。如果要连接到不太安全的网络，为了保护服务器的安全，可启用【阻止所有传入连接】复选框，就可以阻止所有的程序与网络进行通信。选中【关闭】单选按钮，则将禁用 Windows 防火墙。



图 4-9　Windows 防火墙

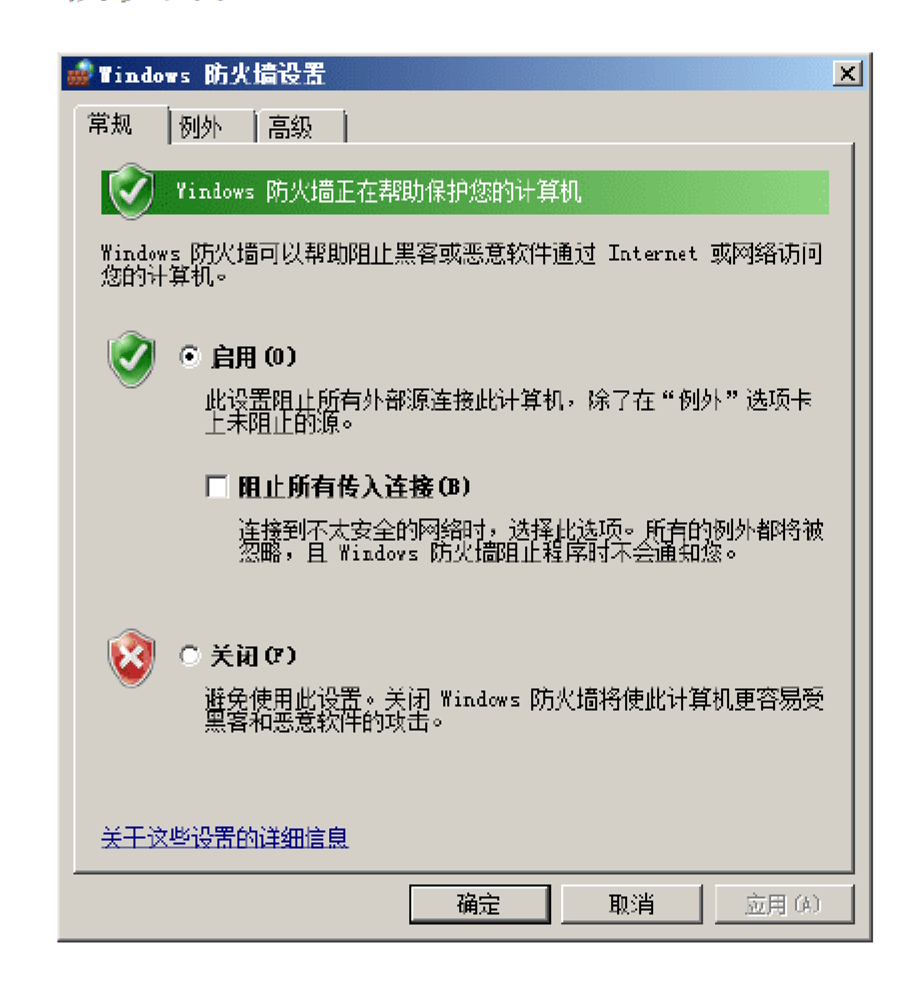


图 4-10　Windows 防火墙设置

4.3　安全配置向导

安装系统补丁、启用 Windows 防火墙可以从一定程度上确保服务器系统的安全性，但是对服务器上安装的应用程序、服务器角色起不到任何保护作用。因此，在完成相应的网络服务器部署之后，管理员还应借助 Windows Server 2008 提供的安全配置向导（SCW），为指定服务或网络应用设置安全配置策略。

4.3.1　安全配置向导概述

安全配置向导（Security Configuration Wizard，SCW）是 Windows Server 2008 附带的一个用于缩小计算机受攻击面的工具。通过 SCW 管理员可以根据服务器角色所需的最少功能来快速完成创建、编辑、应用安全策略等操作。

在 Windows Server 2008 中，已经默认集成安全配置向导，用户无需安装即可直接使用。安全配置向导是一个完全基于服务角色的工具，使用 SCW 创建的安全策略是一个以.xml 结尾的文件，应用后，可以配置服务、网络安全、特定注册表值和审核策略。用户可以根据需要创建针对某个服务器角色的安全策略，并且可以将其应用到其他相应类型的服务器中。例如，服务器可能是文件服务器、打印服务器等。

在配置和应用 SCW 时应该注意如下事项。

- 创建和应用 SCW 安全策略时，应确保服务器的 TCP/IP 属性配置及其端口配置完全正确。
- SCW 禁用不需要的服务并提供对具有高级安全性的 Windows 防火墙的支持。
- 使用 SCW 创建的安全策略与安全模板不同。其中，前者的文件扩展名为.xml；后者的文件扩展名为.inf。用户创建的安全策略源于安全模板，安全模板包含的安全设置可以应用于所有的服务器角色。
- 部署 SCW 安全策略后并不会影响服务器提供服务时所需的组件，并且应用之后，管理员仍可以通过服务器管理器安装所需的组件。
- SCW 不会安装或卸载服务器执行角色时所需的组件。
- 在应用 SCW 安全策略之后，SCW 将自动选择所要从属的角色。
- 在某些情况下，计算机必须连接到 Internet，以使用在 SCW 帮助中所提供的链接。

4.3.2　配置安全策略

利用 SCW 所提供的功能，网络管理员能够非常轻松地完成服务器角色的指定，禁用不需要的服务和端口，配置服务器的网络安全，审核策略、注册表和 IIS 服务器等工作，对巩固服务器的安全有极大的帮助。同时，由于整个配置过程都是在向导对话框中完成的，无需烦琐的手工设置，因此，管理员的工作负担也会得到减轻。

要配置安全策略，首先需要执行【开始】|【管理工具】|【安全配置向导】命令，启动【欢迎使用安全配置向导】对话框，并直接单击【下一步】按钮。然后，在【配置操作】对话框中，选中【新建安全策略】单选按钮，并单击【下一步】按钮，如图 4-11 所示。



图 4-11　新建安全策略

提示　用户也可以单击【开始】菜单，并在【开始搜索】文本框中，输入 scw.exe 命令，按回车键来启动安全配置向导。

在【配置操作】对话框中，为用户提供了 4 种不同的配置操作，每种操作有如下说明。

❑ **新建安全策略**

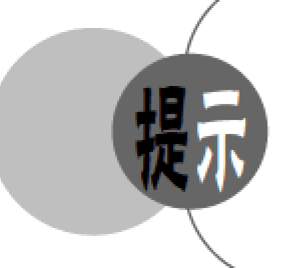
可以创建用于配置服务、Windows 防火墙、Internet 协议安全（IPSec）设置、审核策略和特定注册表设置的安全策略。安全策略文件是 XML 格式的文件，其默认保存路径为%systemroot%\security\msscw\Policies。

❑ **编辑现有安全策略**

可以编辑已使用 SCW 创建的安全策略。只有在选中【编辑现有安全策略】单选按钮的情况下，才能浏览要编辑的安全策略文件所在的文件夹。编辑的策略可存储在本地或网络共享文件夹中。

❑ **应用现有安全策略**

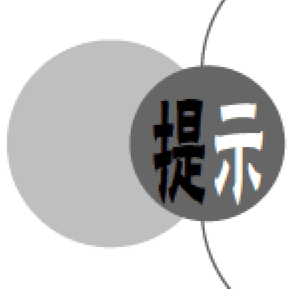
使用 SCW 创建安全策略后，可将其应用到测试服务器，或者应用到生产环境当中。



在将新创建或新修改的安全策略应用到实际生产环境之前，应该首先对其进行测试，然后再将安全策略部署到业务系统当中，测试可使新策略在生产环境中导致意外结果的可能性降至最低。

❑ **回滚上一次应用的安全策略**

如果使用 SCW 应用的安全策略使服务器功能达不到预期所要效果，或者导致其他非预期结果，则可以选中该单选按钮，那么 SCW 将自动从该服务器中删除对应的安全策略。



如果策略是在本地安全策略中编辑的，那么在应用策略后，这些更改就不能回滚到应用前的状态。对于服务和注册表值，回滚过程将会还原在配置过程中更改的设置；对于 Windows 防火墙和 IPSec，回滚过程将会取消当前使用的任何 SCW 策略的分配，并重新分配在配置时使用的前策略。

接着，在弹出的【选择服务器】对话框的【服务器】文本框中，输入需要进行安全配置的 Windows Server 2008 服务器的主机名或 IP 地址。用户也可以通过单击【浏览】按钮选择需要进行安全配置的目标计算机，如图 4-12 所示，然后单击【下一步】按钮。

在【正在处理安全配置数据库】对话框中，用户可以查看到系统正在扫描配置数据库，主要包括已安装或运行的网络服务、IP 地址及子网信息等，当扫描完成后，单击【查看配置数据库】按钮，如图 4-13 所示。

在【SCW 查看器】窗口中，用户可以查看到包括服务器角色、客户端功能、管理和其他选项、服务及 Windows 防火墙的详细信息，如图 4-14 所示。单击【关闭】按钮，在返回到的

【正在处理安全配置数据库】对话框中，单击【下一步】按钮即可。

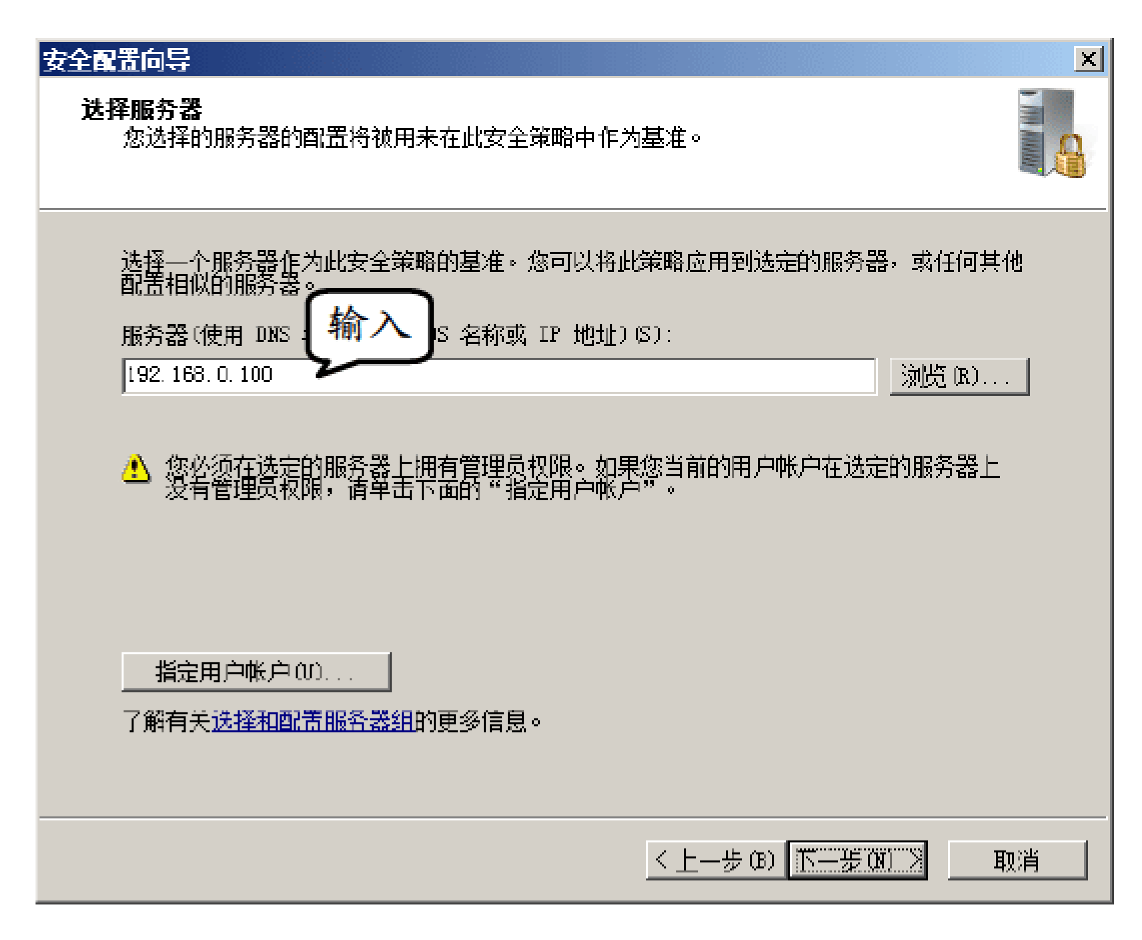


图 4-12　选择配置服务器



图 4-13　安全配置数据库处理完成

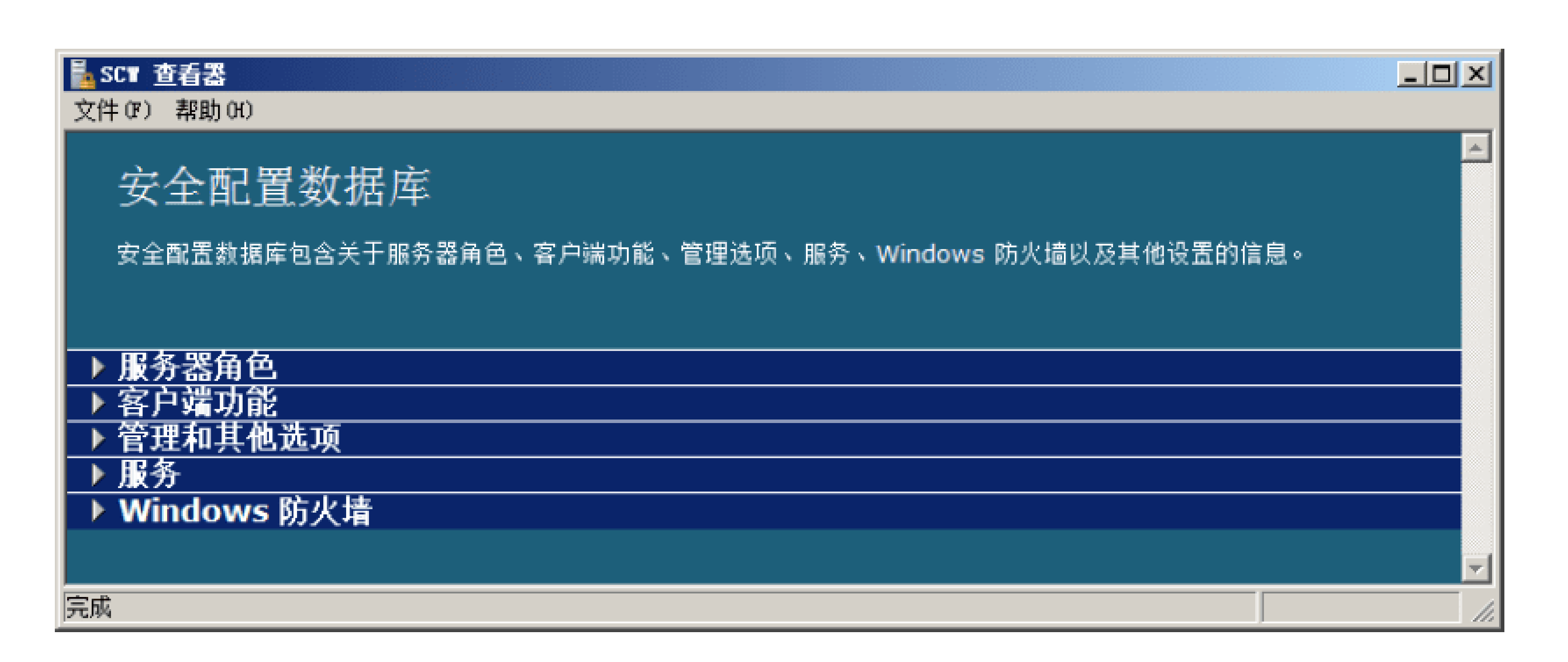
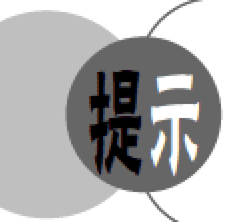


图 4-14　SCW 查看器



在此过程中由于 Internet Explorer 8.0 的安全设置，可能会出现安全提示信息，如果这样则直接单击【是】按钮跳过即可。

在【基于角色的服务配置】对话框中，安全配置向导可以根据当前服务器提供网络服务的不同，配置相应的安全策略，直接单击【下一步】按钮即可，如图 4-15 所示。

在【选择服务器角色】对话框中单击【查看】下拉按钮，在列表中提供了 4 种可供选择的选择模式，默认选择【安装的角色】选项，如图 4-16 所示。当用户选择需要的模式后，单击【下一步】按钮即可。

在该对话框中，对于可供选择的 4 种模式有如下说明。

- **所有角色**　列表内将显示出所有在 Windows Server 2008 中可以使用的角色。
- **安装的角色**　列表内将显示出当前服务器中已经安装的角色，包括没有设置的角色。
- **未安装的角色**　列出当前服务器中没有安装的角色，不包括没有设置的角色。
- **选定的角色**　列出当前服务器中已经选定的角色。

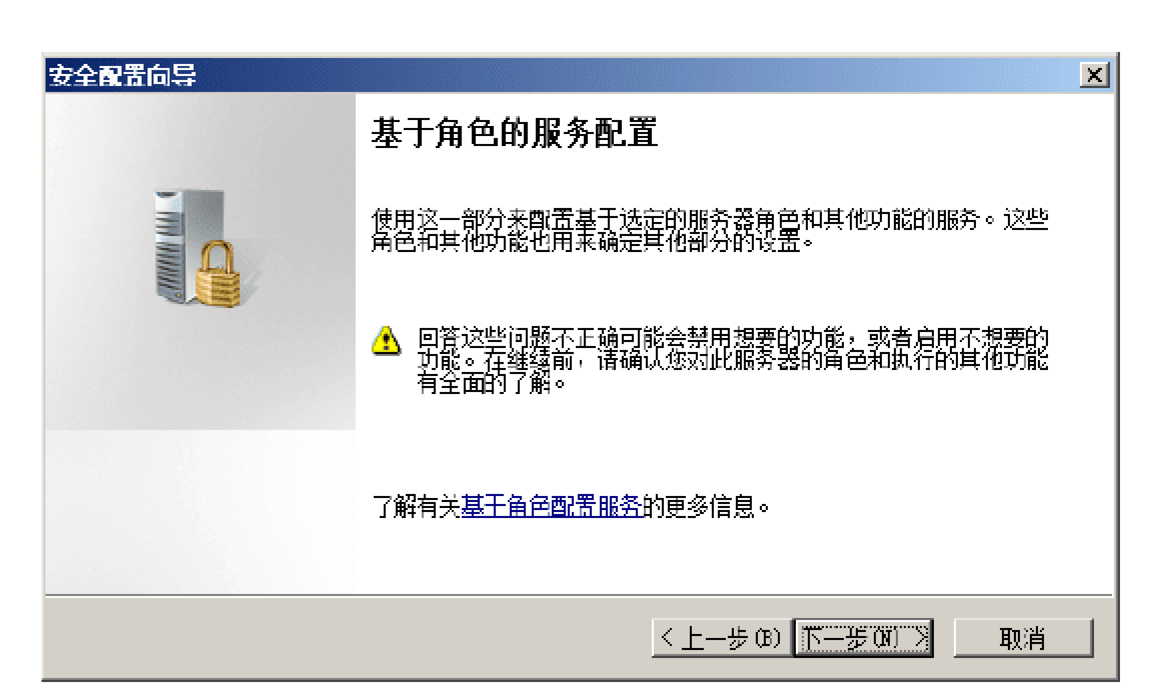


图 4-15　【基于角色的服务配置】对话框



图 4-16　选择服务器角色



为了保证服务器的安全，仅选择所需要的服务器角色即可，如选择多余的服务器角色，会增加 Windows Server 2008 系统的安全隐患。

接下来，在弹出的对话框中依次单击【下一步】按钮，配置其他服务、未指定的服务、确认对服务的更改，从而完成对指定服务器角色的安全策略配置。直到在弹出的【处理未指定的服务】对话框中，选中【不更改此服务的启动模式】单选按钮，并单击【下一步】按钮，如图 4-17 所示。

在该对话框中，提供两种处理未指定服务的方式，每种方式说明如下。

- ❑ **不更改此服务的启动方式**　如果选择该方式，那么在应用此安全策略的服务器上启用的未指定服务将保持启用状态，而禁用的那些服务将保持禁用状态。
- ❑ **禁用此服务**　如果选择该方式，那么不在安全配置数据库中的或未安装在选定服务器上的所有服务都将被禁用。

在弹出的【网络安全】对话框中，开始配置与服务器相关的 Windows 防火墙规则，建议禁用【跳过这一部分】复选框，如图 4-18 所示。然后，单击【下一步】按钮。

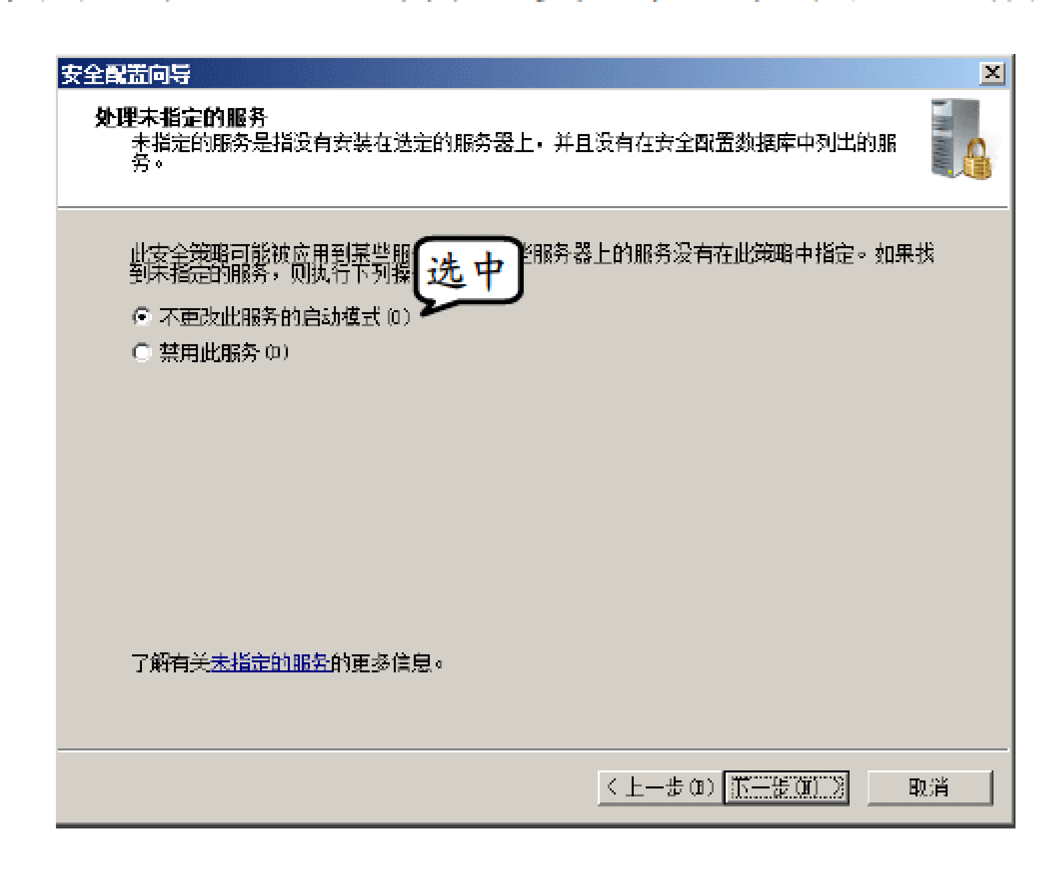


图 4-17　选择未指定服务的处理方式

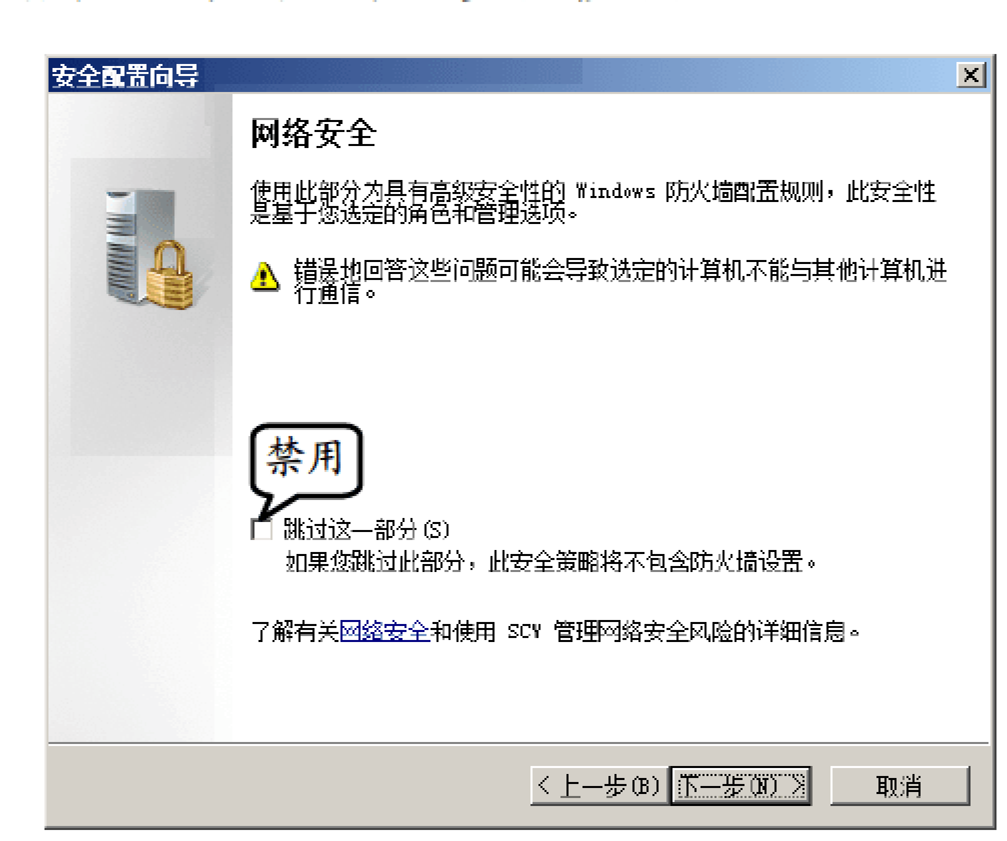
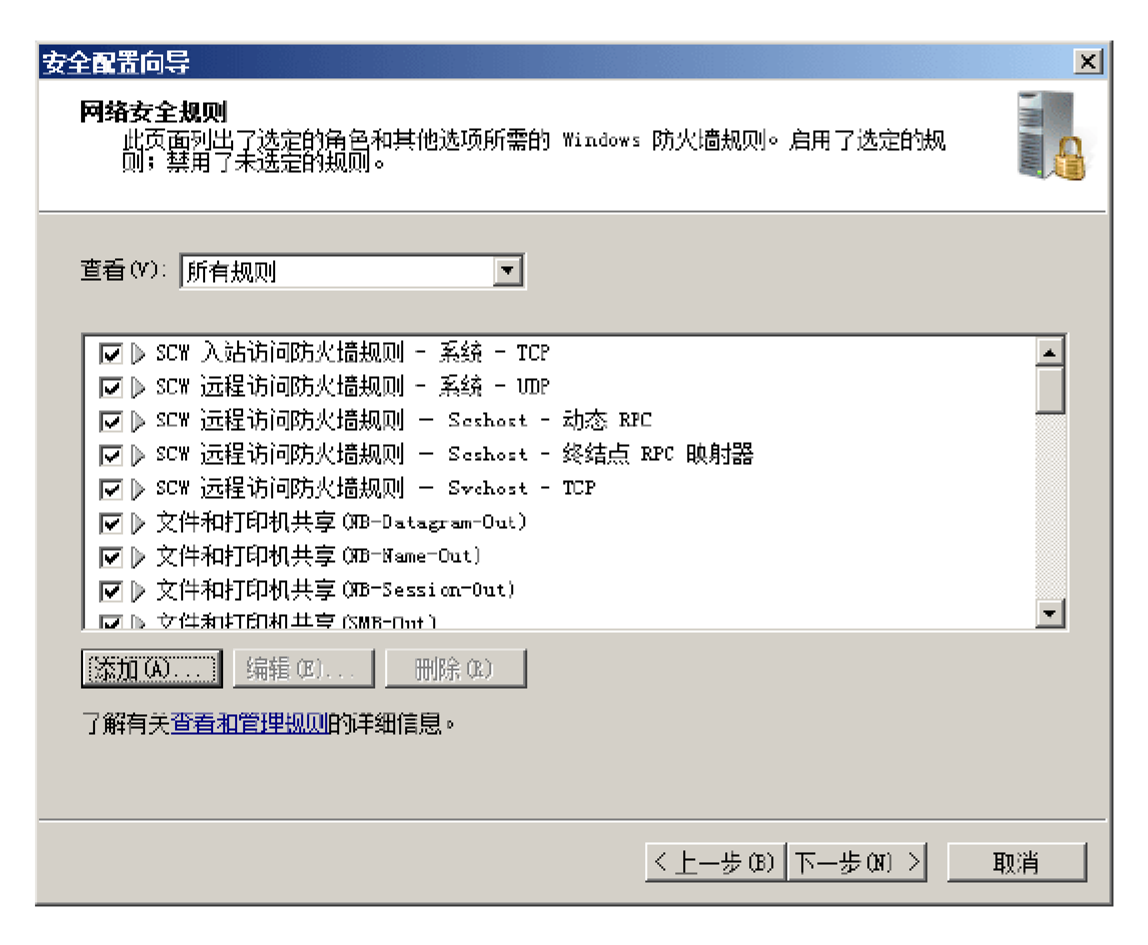


图 4-18　【网络安全】对话框

在【网络安全规则】对话框中，默认显示所有选定角色和其他选项所需的 Windows 防火墙规则，如图 4-19 所示。如果在【网络安全规则】对话框中的列表内没有列出需要使用的 Windows 防火墙规则，则可以单击【添加】按钮。

在弹出的对话框中的【名称】文本框内输入规则名称（如 www），如图 4-20 所示。为了便于区分，还可以输入相关的描述信息。另外，还可以设置限制连接方式。最后，单击【确定】按钮。



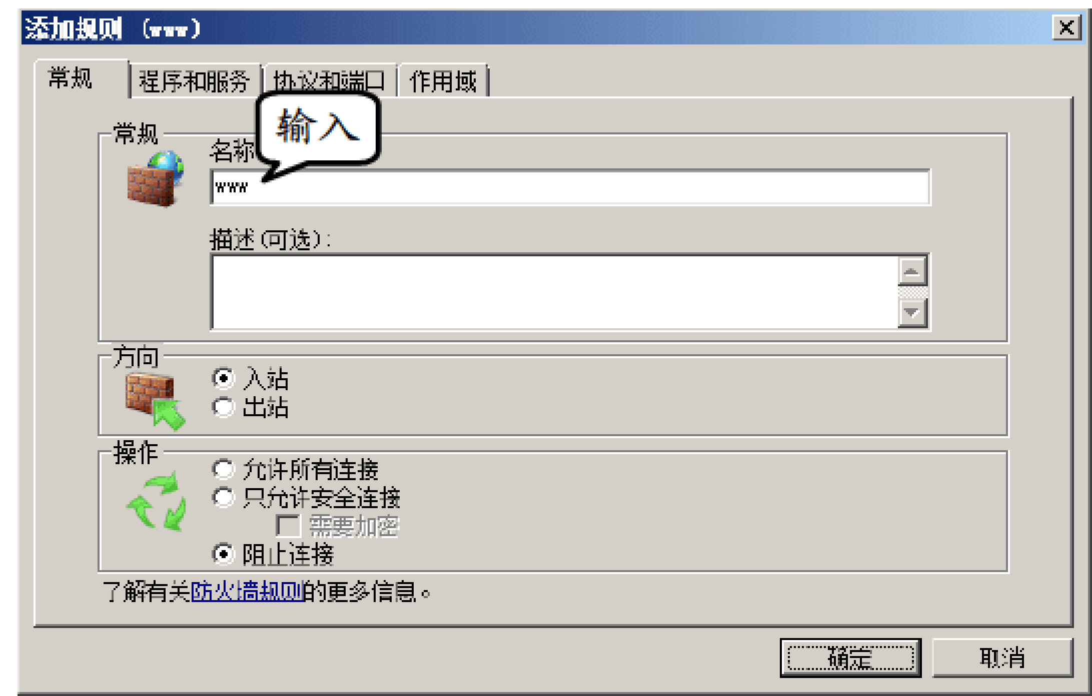


图 4-19　网络安全规则　　　　图 4-20　添加规则

在【注册表设置】对话框中，通过该设置可以修改 Windows Server 2008 服务器注册表中的一些特殊键值，从而严格限制用户的访问权限，建议用户禁用【跳过这一部分】复选框，单击【下一步】按钮，如图 4-21 所示。

在【要求 SMB 安全签名】对话框中，可以配置 SMB 安全签名选项，默认已启用【所有连接到它的计算机满足下列最低操作系统要求】和【它有剩余的处理器能力，可以用来给文件和打印通讯签名】复选框，如图 4-22 所示。然后，单击【下一步】按钮。

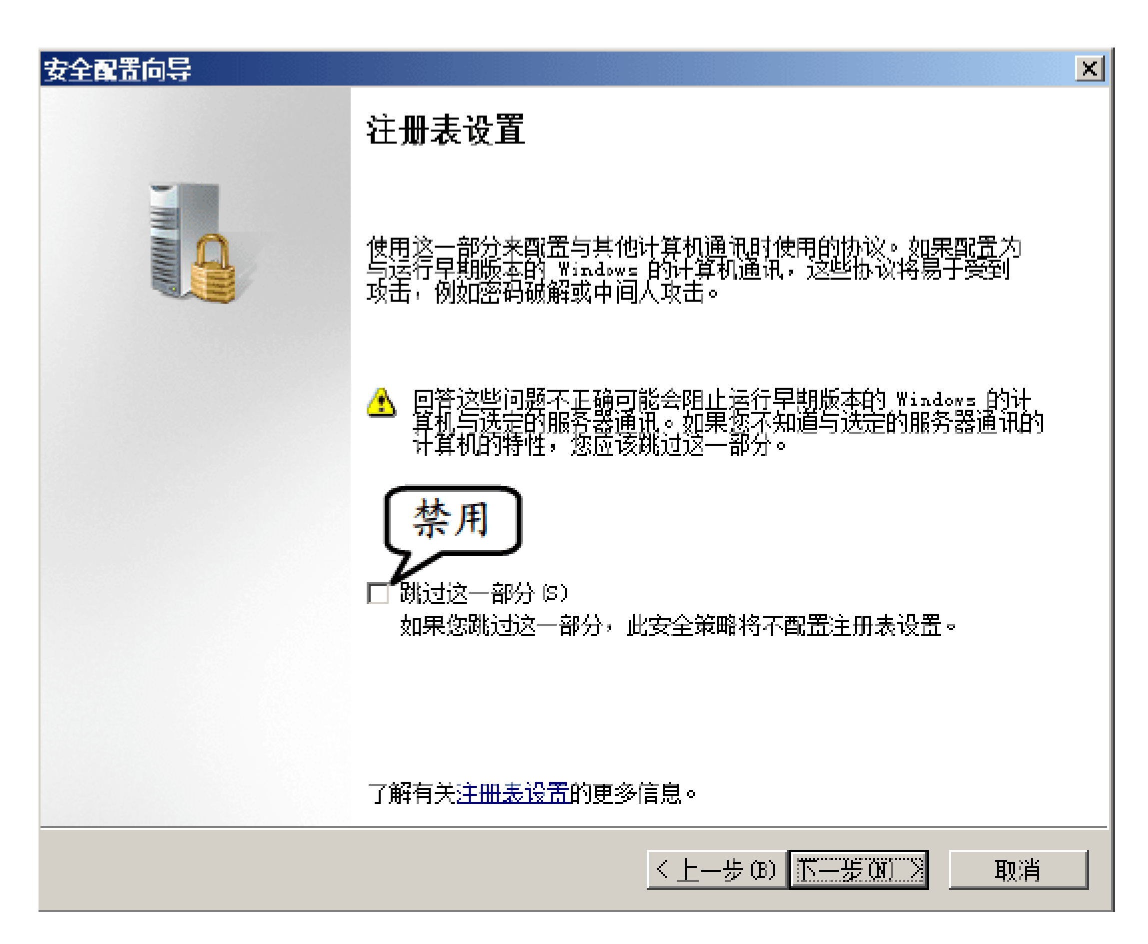
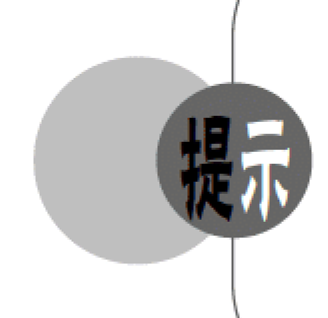




图 4-21　注册表设置　　　　图 4-22　设置 SMB 安全签名



SMB 协议为 Microsoft 文件和打印共享以及许多其他网络操作（如远程管理）提供基础。SMB 协议支持 SMB 数据包的数字签名。此策略设置确定在允许与 SMB 客户端进行进一步通信之前，是否必须协商 SMB 数据包签名。如果启用此设置，除非 Microsoft 网络客户端同意进行 SMB 数据包签名，否则，网络服务器不会与该客户端进行通信。

在【出站身份验证方法】对话框中，如果是在域网络中进行远程登录，那么启用【域账户】复选框即可；如果是工作组环境，则启用【远程计算机上的本地账户】复选框，并单击【下一步】按钮，如图 4-23 所示。

在【出站身份验证使用本地账户】对话框中，启用【Windows NT 4.0 Service Pack 6a 或更新的操作系统】复选框，并单击【下一步】按钮，如图 4-24 所示。在该对话框中对这两种属性有如下说明。



图 4-23　设置出站身份验证方法



图 4-24　【出站身份验证使用本地账户】对话框

- **Windows NT 4.0 Service Pack 6a 或更新的操作系统**

用于确定连接到该服务器的客户端支持身份验证。运行 Windows NT 4.0 Service Pack 4（SP4）以及更低版本的计算机不支持身份验证。另外，运行 Windows 95 和 Windows 98 的计算机不支持身份验证。

- **与选定的服务器的时钟进行同步的时钟**

检查客户端是否满足使用身份验证的要求。身份验证需要进行同步。较旧的系统不使用时钟同步。如果网络只包含运行 Windows 2000、Windows XP 或 Windows Server 2003 的计算机，则表示用户的环境会使用时钟同步。

在弹出的【注册表设置摘要】对话框中，确认注册表设置正确无误后直接单击【下一步】按钮。在【审核策略】对话框中，Windows 审核策略主要用于审核日志记录中的相关内容，并确定受影响的系统对象。安全策略回滚功能是无法回滚安全向导中的审核策略设置的。建议用户禁用【跳过这一部分】复选框，单击【下一步】按钮，如图 4-25 所示。

在【系统审核策略】对话框中，选中【审核成功的操作】单选按钮，并单击【下一步】按钮，如图 4-26 所示。在该对话框中包括 3 种审核目标，每种审核目标有如下说明。



图 4-25 【审核策略】对话框

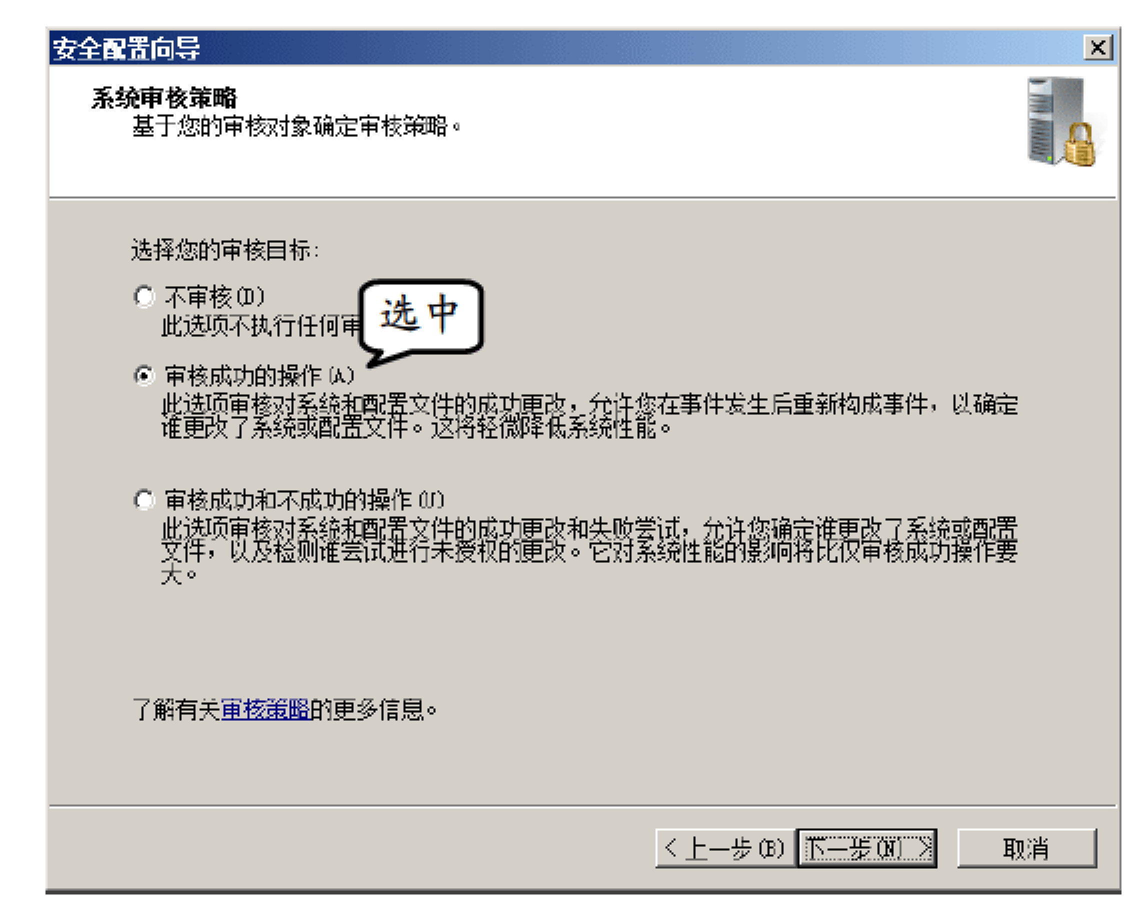
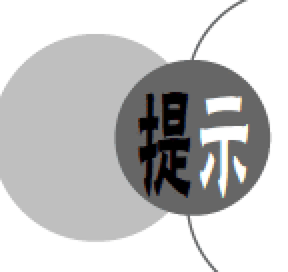


图 4-26 选择审核目标

- ❑ **不审核** 不执行任何审核。CPU 周期和磁盘空间空闲下来，以便可以提高其他进程的性能。
- ❑ **审核成功的操作** 与审核成功和不成功的操作相比，审核成功的操作可以减少事件日志的项数。使用此选项将只记录用户实际访问的内容，而不记录用户尝试访问的内容。
- ❑ **审核成功和不成功的操作** 用户除了要使用审核事件来记录成功完成的事件之外，还要记录用户对无权访问区域的尝试事件。



除非用户需要定期查看安全日志，否则，不要选中【审核成功和不成功的操作】单选按钮。如果用户尝试访问无权访问的资源，可能会产生许多失败审核，从而填满安全日志，当安全日志被填满后，将覆盖最早的审核项。

在【审核策略摘要】对话框中，确保审核选择正确无误后，单击【下一步】按钮，如图 4-27 所示。

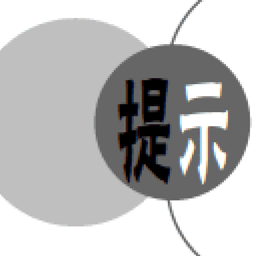
在【保存安全策略】对话框中，直接单击【下一步】按钮，在弹出的【安全策略文件名】对话框中，设置安全策略文件名及保存路径，如图 4-28 所示。然后，单击【下一步】按钮。



图 4-27 查看审核策略摘要信息



图 4-28 设置安全策略文件名及路径



单击【包括安全模板】按钮，还可以向当前安全策略中添加其他安全模板中的安全规则，这些规则将拥有较高的优先级。SCW 回滚功能将无法回滚已经应用的策略模板中的规则设置。

在【应用安全策略】对话框中，如果选中【现在应用】单选按钮，可以将安全策略立即应用到当前服务器，但建议选中【稍后应用】单选按钮，当该安全策略测试之后再应用到服务器。然后，单击【下一步】按钮，如图 4-29 所示。最后，在弹出的对话框中单击【完成】按钮，完成安全策略的设置。

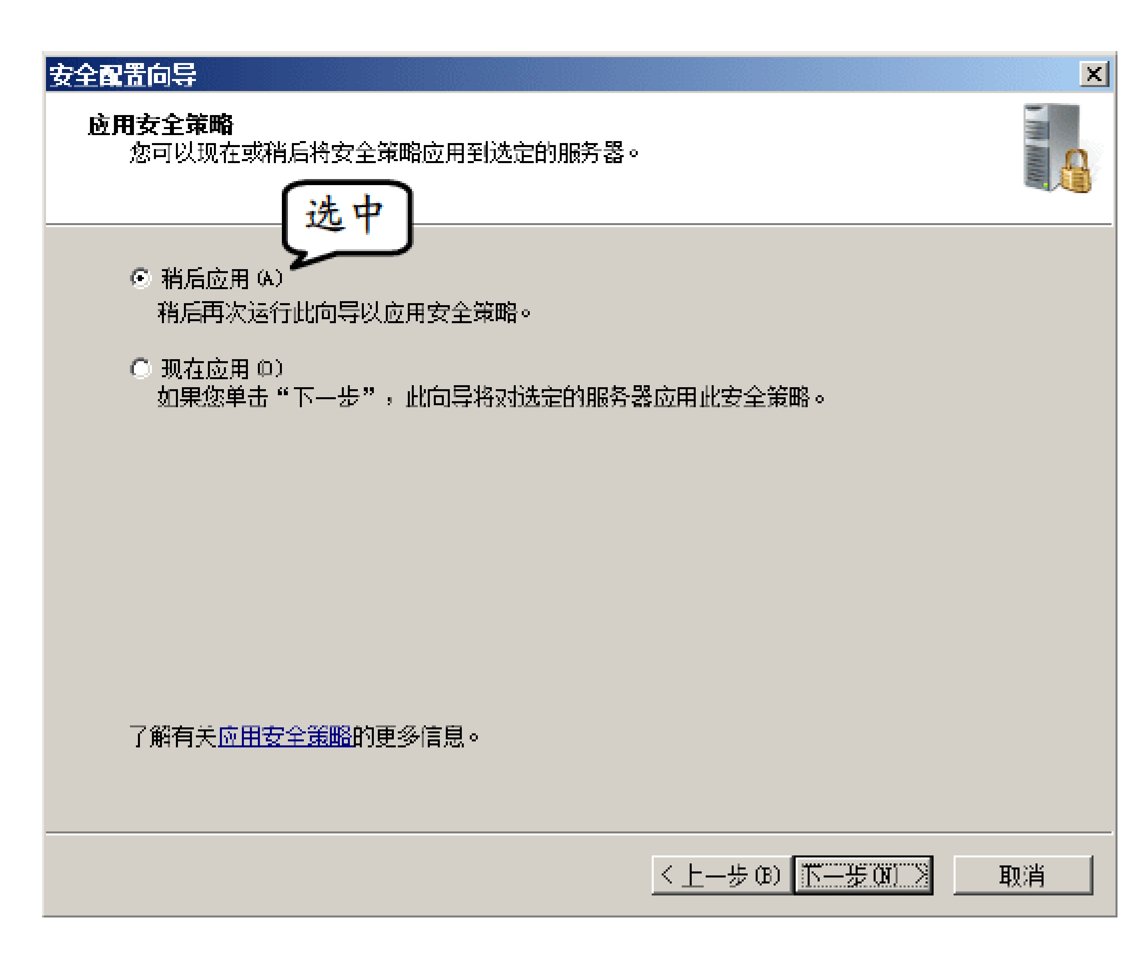


图 4-29　稍后应用安全策略

4.3.3　应用安全配置策略

使用安全配置向导创建的安全策略，可以直接应用于所有运行 Windows Server 2008 或者 Windows Server 2003 SP1/SP2/R2 操作系统的网络服务器。但在大规模应用安全策略之前必须对其进行严格的测试，确认可行之后方可进行部署及应用。在应用安全策略之后，必须重启计算机才能使安全配置策略生效。

要应用安全配置策略，需要执行【开始】|【管理工具】|【安全配置向导】命令，在弹出的对话框中直接单击【下一步】按钮。然后，在【配置操作】对话框中，选中【应用现有安全策略】单选按钮，并通过单击【浏览】按钮，选择现有安全策略文件，如图 4-30 所示。然后，单击【下一步】按钮。

在【选择服务器】对话框中的【服务器】文本框内输入安全策略的名称或 IP 地址。如果目标服务器为远程主机，则应单击【指定用户账户】按钮，选择连接到指定主机部署安全策略所使用的用户账户及凭证。然后，单击【下一步】按钮，如图 4-31 所示。



图 4-30　设置配置操作

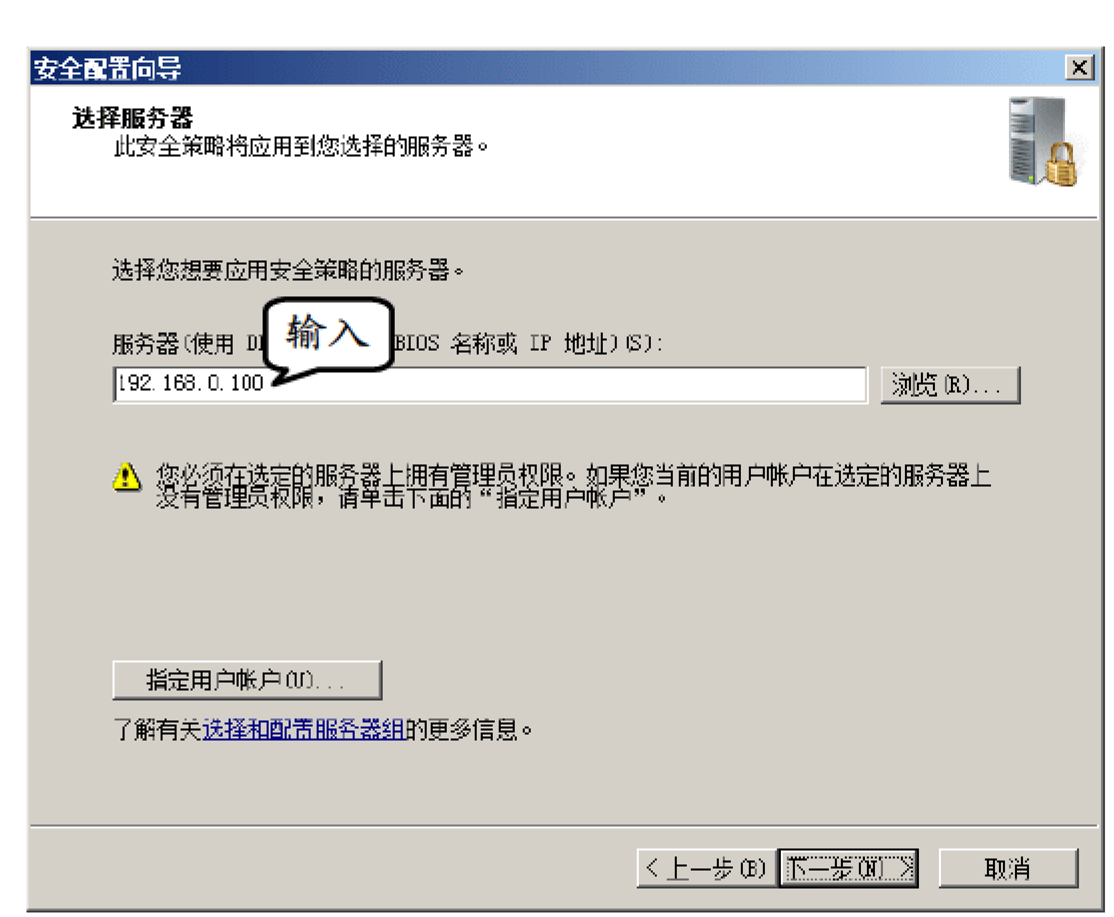
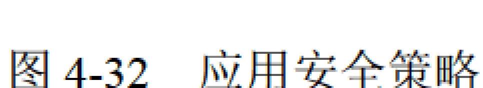


图 4-31　选择服务器

在【应用安全策略】对话框中，通过单击【查看安全策略】按钮，可以查看所选安全策略的描述信息，在查看之后单击【下一步】按钮即可，如图 4-32 所示。

将安全策略应用到本地计算机大概需要几分钟时间，应用到远程计算机中所需要的时间可能更长一些，当应用完成后，直接单击【下一步】按钮即可。然后，在【正在完成安全配置向导】对话框中，直接单击【完成】按钮，如图 4-33 所示。最后，重新启动计算机，使应用的安全策略生效即可。




图 4-32　应用安全策略

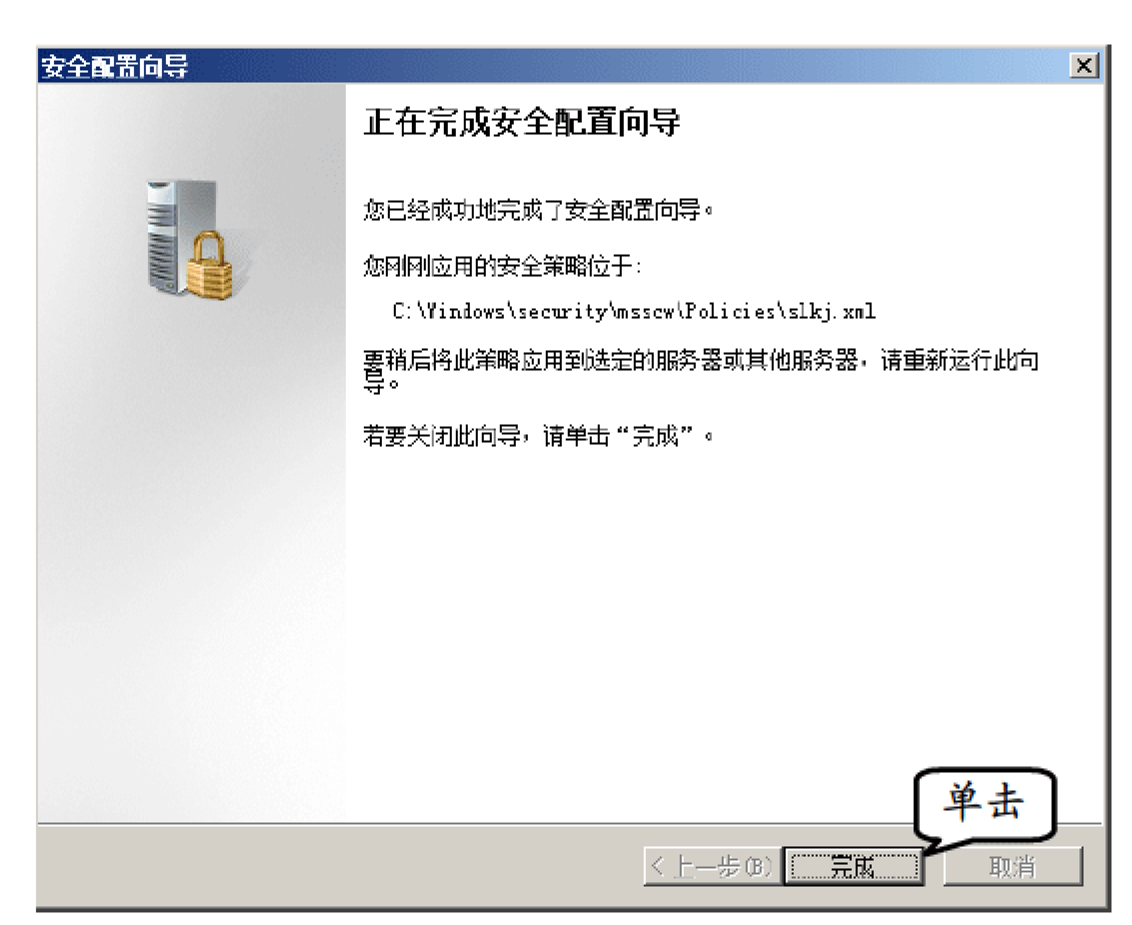


图 4-33　完成安全配置向导

4.4　默认共享

默认共享是在系统安装完毕后就自动开启的共享，也叫管理共享，常被管理员用于远程管理计算机。但是，对个人用户来说默认共享有时是不安全的，如果计算机联网，那么网络上的一些黑客可以通过连接用户的计算机实现对这些默认共享的访问。因此，需要用户合理地管理默认共享。

4.4.1　查看默认共享

在 Windows 2000/XP 及更高的版本的操作系统中，默认开启的共享包括“C$”、“D$”等所有的逻辑盘以及“admin$”和“ipc$”，这些共享都有“$”标志，表示是隐含的。用户可以在【运行】对话框中输入“\\计算机名\盘符$”对这些默认共享资源进行访问。如果要查看默认共享资源可以通过如下两种方法实现。

1．使用 net share 命令

首先，执行【开始】|【运行】命令，在弹出的【运行】对话框中，输入 cmd 命令，并单击【确定】按钮，如图 4-34 所示。

在【管理员：命令提示符】窗口中，输入 net share 命令，并按回车键，即可查看到所有

默认共享资源，如图 4-35 所示。

图 4-34　输入 cmd 命令

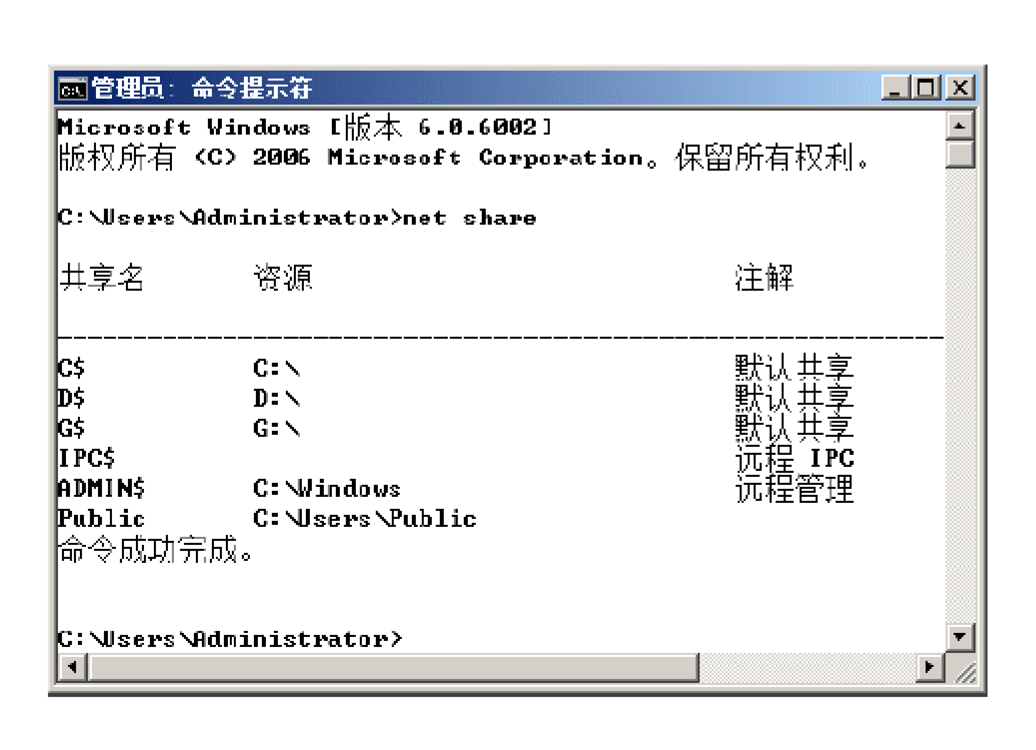


图 4-35　查看默认共享

2. 使用计算机管理

首先执行【开始】|【管理工具】|【计算机管理】命令，在【计算机管理】窗口中展开【共享文件夹】节点，并单击【共享】选项。然后，在右侧窗格中即可查看到默认共享资源，如图 4-36 所示。

4.4.2　停止默认共享

默认共享主要是为了方便网络管理员管理网络中的计算机，特别是在基于域环境的网络当中，专门有几个默认共享用于存储用户配置文件，是非常方便的。但是，默认共享在方便管理员管理的同时，也给计算机带来了安全隐患。如果知道了管理员的账号和密码，那么任何人都能够访问计算机，所以如果管理员账户和密码被恶意用户窃取，对于计算机的安全性来讲是非常不利的。如果在网络中没有使用默认共享的必要，建议用户将系统的默认共享关闭，从而进一步保证计算机的安全性。

1. 使用 net share 命令停止默认共享

与查看默认共享基本相同，以管理员身份打开【管理员：命令提示符】窗口，输入 net share ADMIN$ /DELETE 命令，并按回车键，可查看到 ADMIN$已经删除信息，如图 4-37 所示。



图 4-36　【计算机管理】窗口

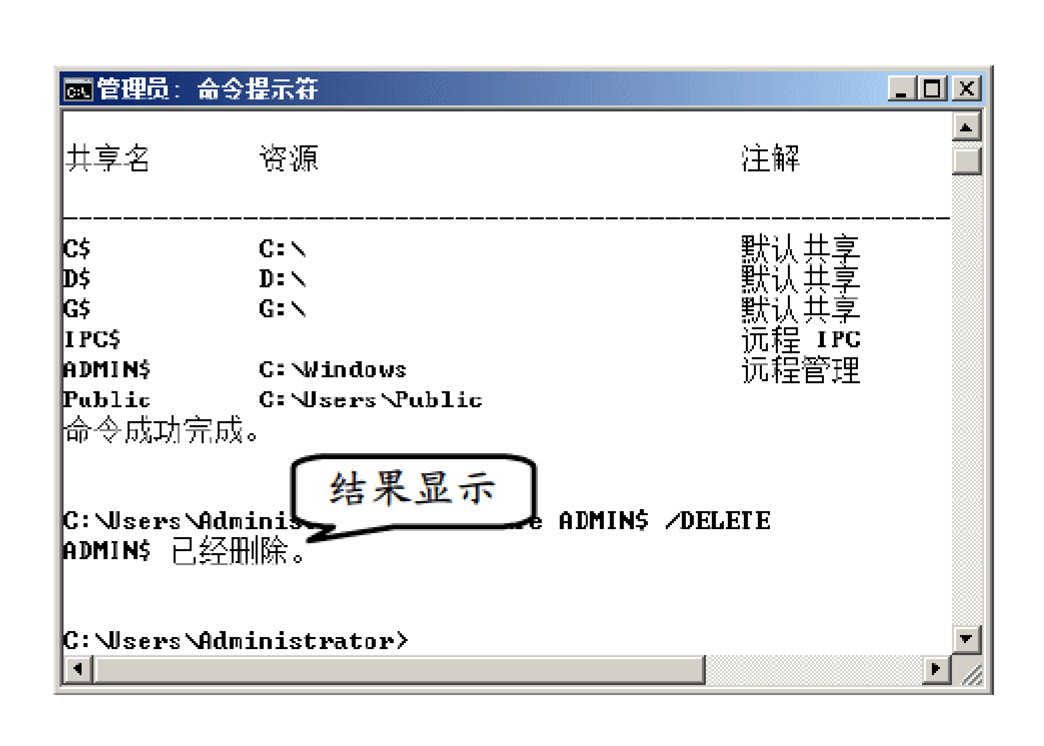
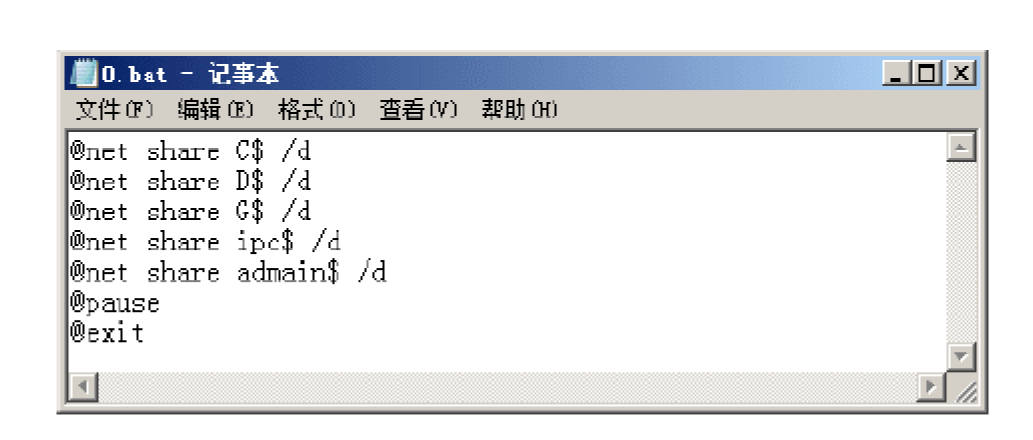


图 4-37　删除 ADMIN$默认共享

使用同样的方法，还可以删除 C$、D$、G$、IPC$等默认共享。在“/DELETE”前必须要有空格。另外，可以使用“net share ADMIN$”命令或“net share IPC$”命令建立“ADMIN$”或“IPC$”共享（如果共享存在，则为显示共享），但是，其他共享则不能通过该方法来建立默认共享。

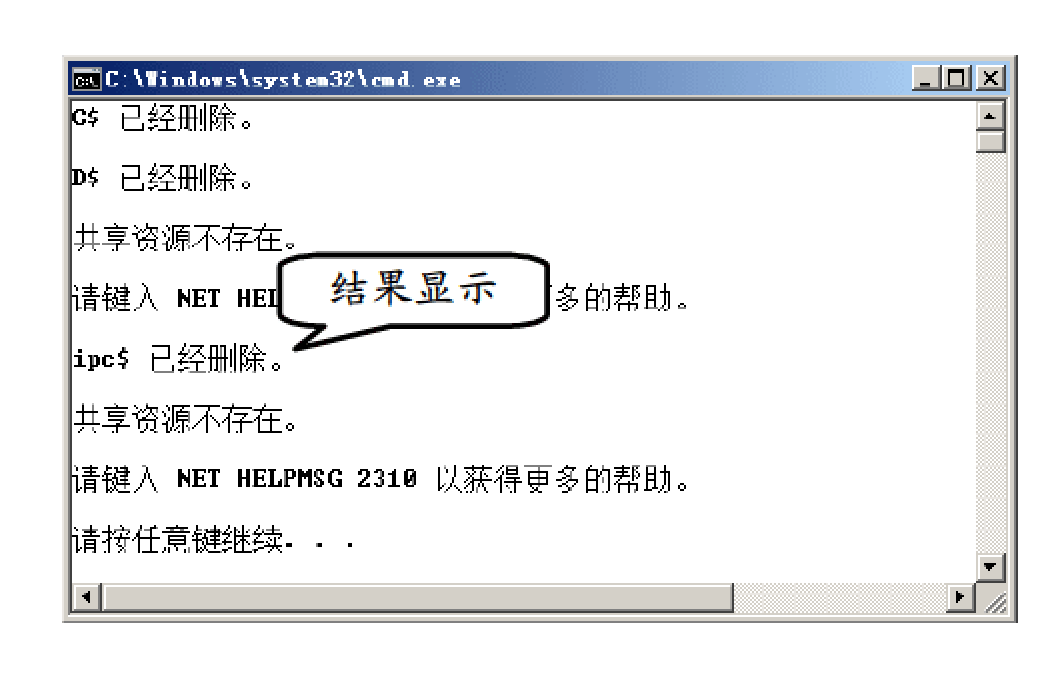
如果需要删除所有的默认共享，还可以使用脚本命令（批处理文件方式）来完成，即建立一个.bat 文件，在该文件中输入如下内容，如图 4-38 所示。

然后，双击该.bat 文件，在弹出的【命令提示符】窗口中，即可查看到所有默认共享都被删除的信息，如图 4-39 所示。




```
@net share C$ /d
@net share D$ /d
@net share G$ /d
@net share ipc$ /d
@net share admain$ /d
@pause
@exit
```

图 4-38　批处理文件内容




```
C$ 已经删除。
D$ 已经删除。
共享资源不存在。
请键入 NET HEL...多的帮助。
ipc$ 已经删除。
共享资源不存在。
请键入 NET HELPMSG 2310 以获得更多的帮助。
请按任意键继续. . .
```

图 4-39　通过批处理文件删除默认共享

用户可以根据需要分别删除默认共享的盘符，该批处理文件可以通过双击执行，也可以在命令提示符下运行或者添加到启动项中。

2. 关闭 Server 服务停止默认共享

默认共享使用的是计算机系统的 Server 服务，如果将该服务关闭，就可以直接删除默认共享。

首先，执行【开始】|【管理工具】|【服务】命令，在打开的【服务】窗口中，右击 Server 选项，并执行【属性】命令，如图 4-40 所示。

在弹出的【Server 的属性（本地计算机）】对话框中，单击【启动类型】下拉按钮，选择【禁用】选项，然后，单击【停止】按钮，如图 4-41 所示。最后，单击【确定】按钮。

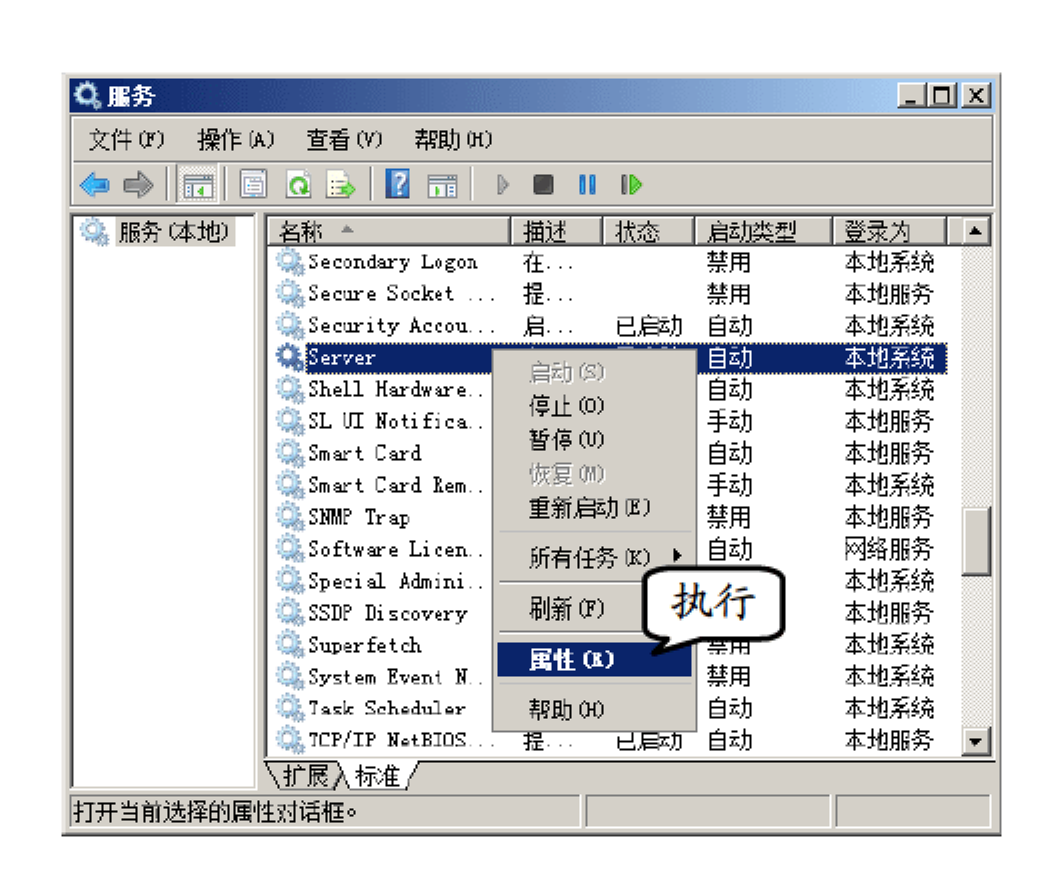


图 4-40　服务窗口



图 4-41　禁用 Server 服务

再次打开【命令提示符】窗口，输入 net share 命令，并按回车键，可看到 Server 服务没有启动的提示，此时直接输入“n”，按回车键退出即可，如图 4-42 所示。

即使用户输入“y”，也会查看到无法启动该服务的提示。另外，使用这种方法停止默认共享后，其他共享也将同时被取消。

3. 修改注册表

使用 net share 命令和关闭 Server 服务停止默认共享时，当系统重新启动后，默认共享会重新恢复。如果用户需要永久性地停止系统默认共享，可以通过修改注册表的方法来实现该目的。停止系统默认共享的键值，在默认情况下的 Windows 操作系统上并不存在，需要用户手动添加该键值，修改后重新启动计算机使该键值生效即可。

首先，执行【开始】|【运行】命令，在弹出的对话框中输入 regedit 命令，并单击【确定】按钮，如图 4-43 所示。



图 4-42　关闭 Server 服务后

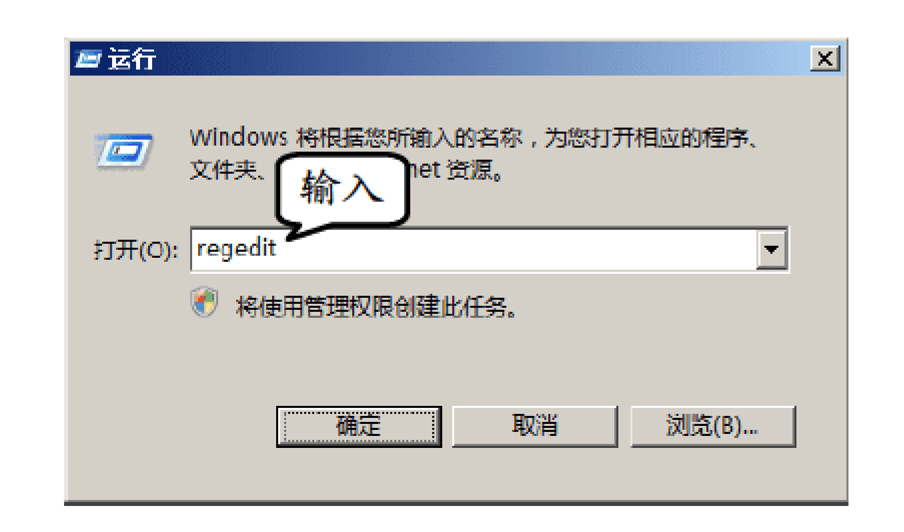


图 4-43　输入 regedit 命令

在打开的【注册表编辑器】窗口中，依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer 节点，并选择 AutotunedParameters 选项。然后，在右侧窗格的任意空白位置右击，并执行【新建】|【DWORD（32 位）值】命令，如图 4-44 所示。

新建一个名为 Autoshareserver 的 DWORD 值，并将其赋值为“00000000”，如图 4-45 所示。



图 4-44　【注册表编辑器】窗口



图 4-45　创建 DWORD 值

4.4.3　设置隐藏共享

通常，用户可以通过网上邻居查看或者访问其他计算机上的共享资源，但其中并不包括

隐藏共享。因此，设置隐藏共享也是保护共享资源安全的一种常用方法。这里访问者必须使用准确的共享名才可以访问。

在【计算机】窗口中，右击想要设置隐藏共享的文件夹（以 backup 文件夹为例），并执行【属性】命令，如图 4-46 所示。

在弹出的对话框中切换到【共享】选项卡，并单击【高级共享】按钮，如图 4-47 所示。



图 4-46　执行【属性】命令

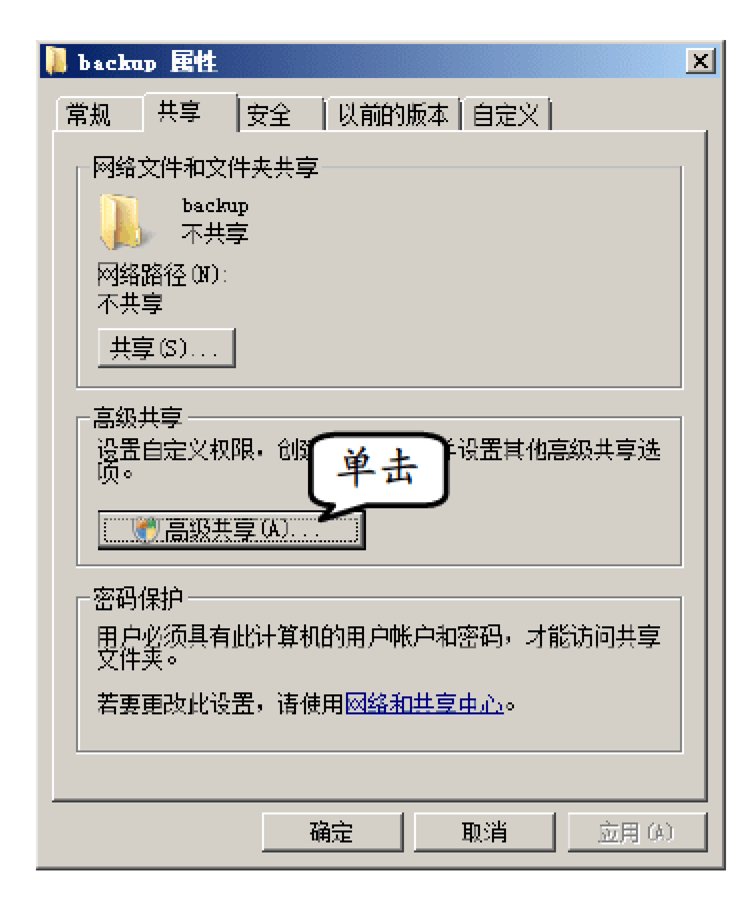


图 4-47　【backup 属性】对话框

在【高级共享】对话框中启用【共享此文件夹】复选框，并在【共享名】文本框中显示的默认名称后追加“$”，如图 4-48 所示。当然，也可以设置其他共享名，但隐藏共享必须以“$”结尾。

网络中的其他计算机无法直接通过资源管理器访问隐藏共享，然而可以在任意地址栏中输入“\\服务器\共享名”进行访问，但此时的共享名中也包括特殊字符“$”，如输入“\\192.168.0.100\backup$”即可访问该隐藏共享文件中的内容，如图 4-49 所示。



图 4-48　设置隐藏共享

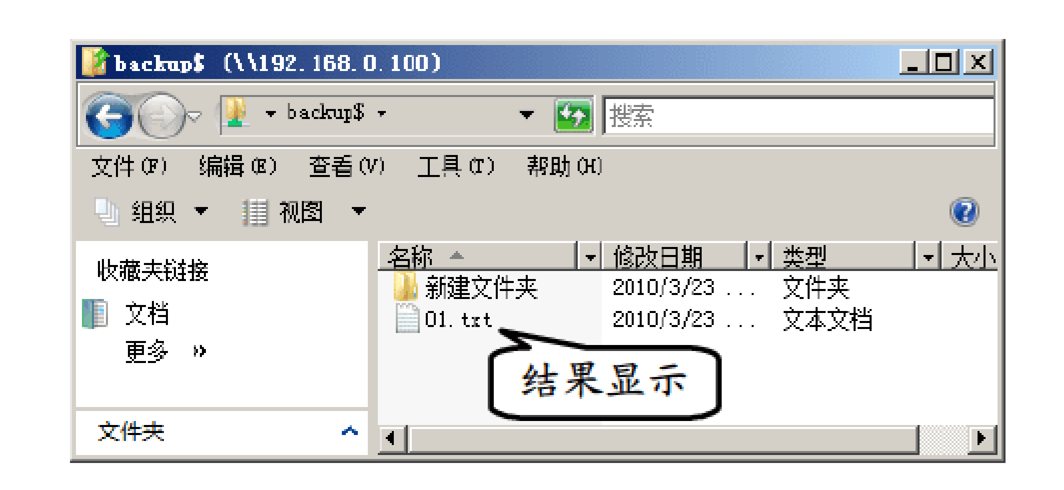


图 4-49　查看隐藏共享文件内容

4.4.4　网管心得——系统服务配置注意事项

任何网络服务的安装都建立在系统服务的基础上，因此做好系统服务安全是系统安全和网络安全的重要环节。任何服务都可能存在漏洞，但也不能因此而置之不理，最好的方案就是通过一切可行方法，确保系统服务的安全，如禁用非必要的服务、设置服务访问权限等。

在配置系统服务时应注意以下事项。

- 根据服务的描述及业务的需求，确定是否使用该服务。
- 具体到每个服务的内容和功能，需要参考微软的说明及咨询业内安全专家。
- 禁止或者设置成手动启动的方式处理系统非必要的服务。
- 如对系统可能造成的影响不了解，那么应该在测试环境中测试验证通过之后，再在应用环境中部署。
- 对于安装应用程序时同步安装的服务，如果没有必要，应该将其关闭。

在 Windows Server 2008 中，通过执行【开始】|【管理工具】|【服务】命令，在打开的【服务】窗口中，可以查看到本地计算机中所有的服务，如图 4-50 所示。

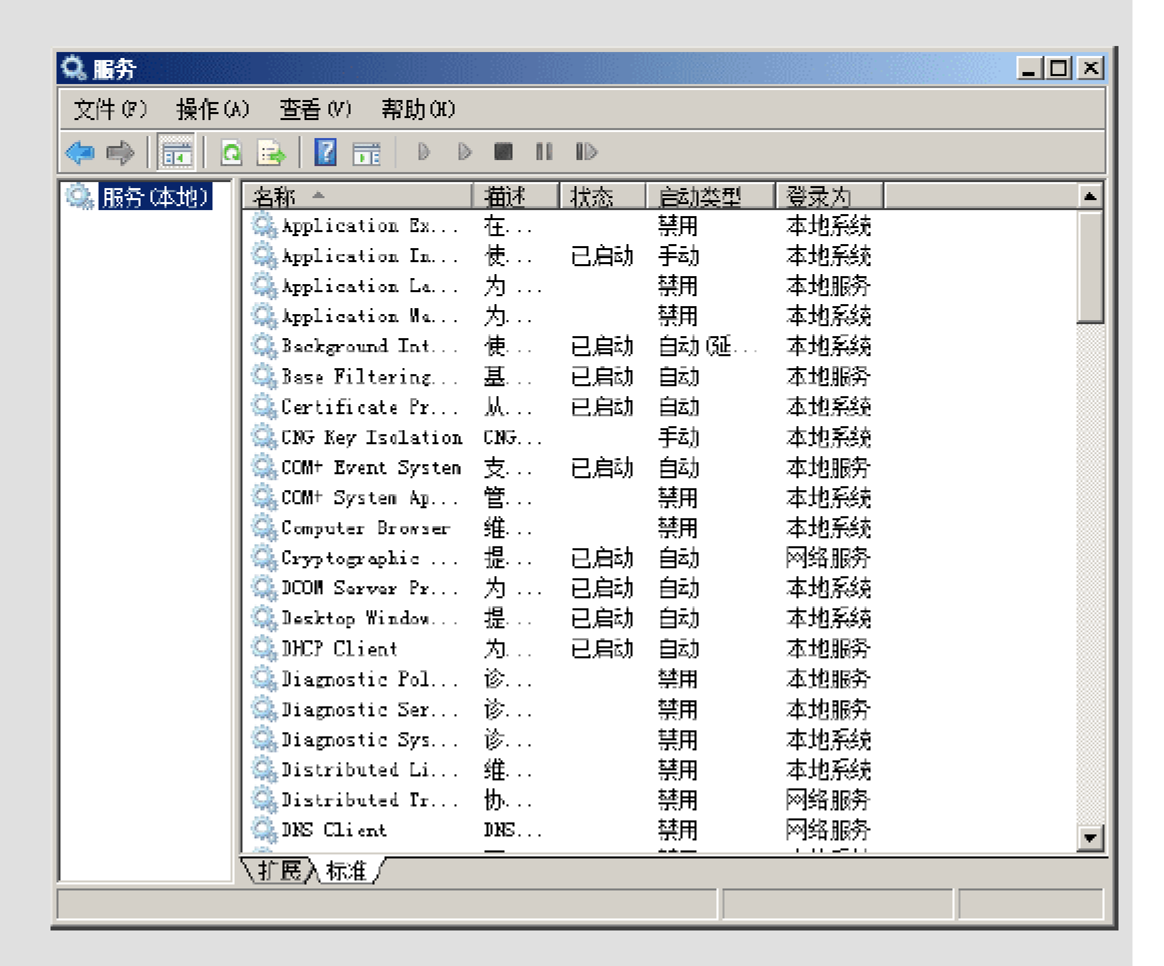


图 4-50　本地计算机默认服务列表

对于系统服务的处理不同于其他设置，因为所有服务的漏洞、对策及潜在影响在本质上都一样。安装 Windows Server 2008 操作系统时，系统在启动时创建并配置默认服务。其中，有些服务在组织环境中并不需要，但在 Windows 中仍被启用，用于确保应用程序或客户端的兼容性或者辅助进行系统管理。

4.5　操作实例

4.5.1　操作实例——使用本地安全策略禁用端口服务

Windows 中每一项服务都对应相应的端口，如 WWW 服务的端口是 80，ftp 服务的端口是 21，使用【本地安全策略】命令禁用不必要的端口，控制端口服务，可有效地提升计算机安全，不被黑客入侵。

1. 实例目的

- 创建 IP 安全策略。
- 筛选数据包。
- 加固系统，保护系统安全。

2. 实例步骤

（1）在桌面执行【开始】|【程序】|【管理工具】|【本地安全策略】命令，在打开的窗口中，右击左侧窗格中的【IP 安全策略，在本地计算机】选项，并执行【创建 IP 安全策略】命令，如图 4-51 所示。

（2）在弹出的【IP 安全策略向导】对话框中，单击【下一步】按钮，如图 4-52 所示。

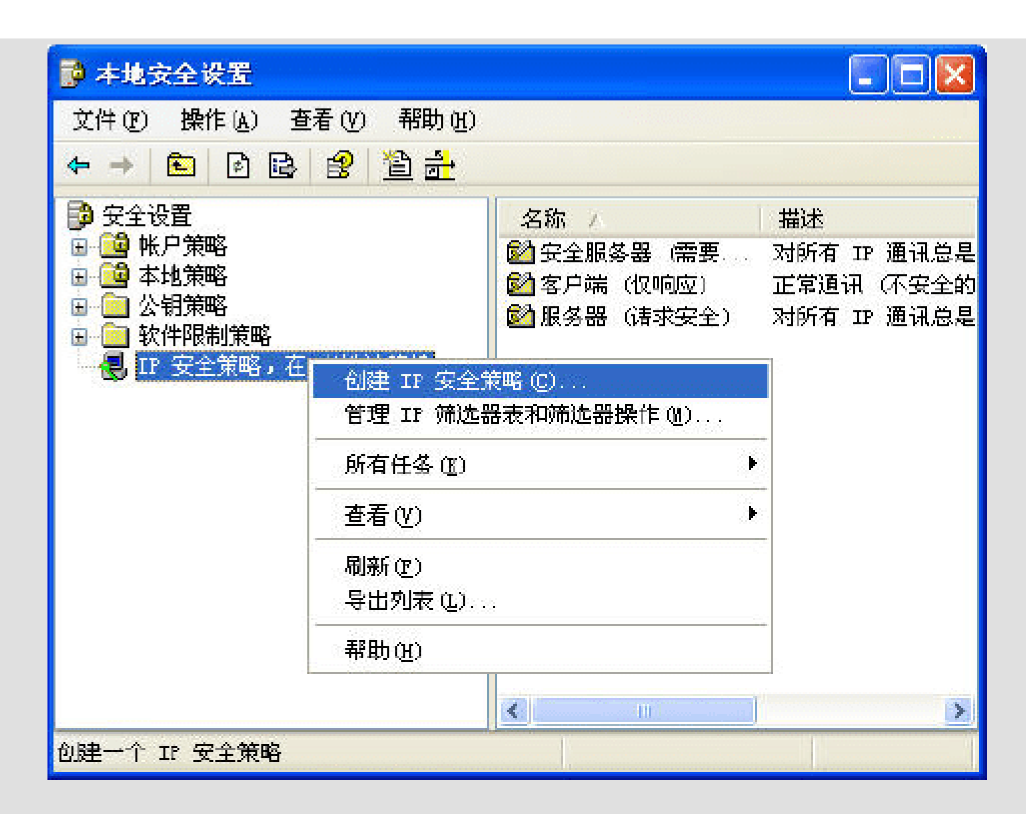


图 4-51　创建 IP 安全策略

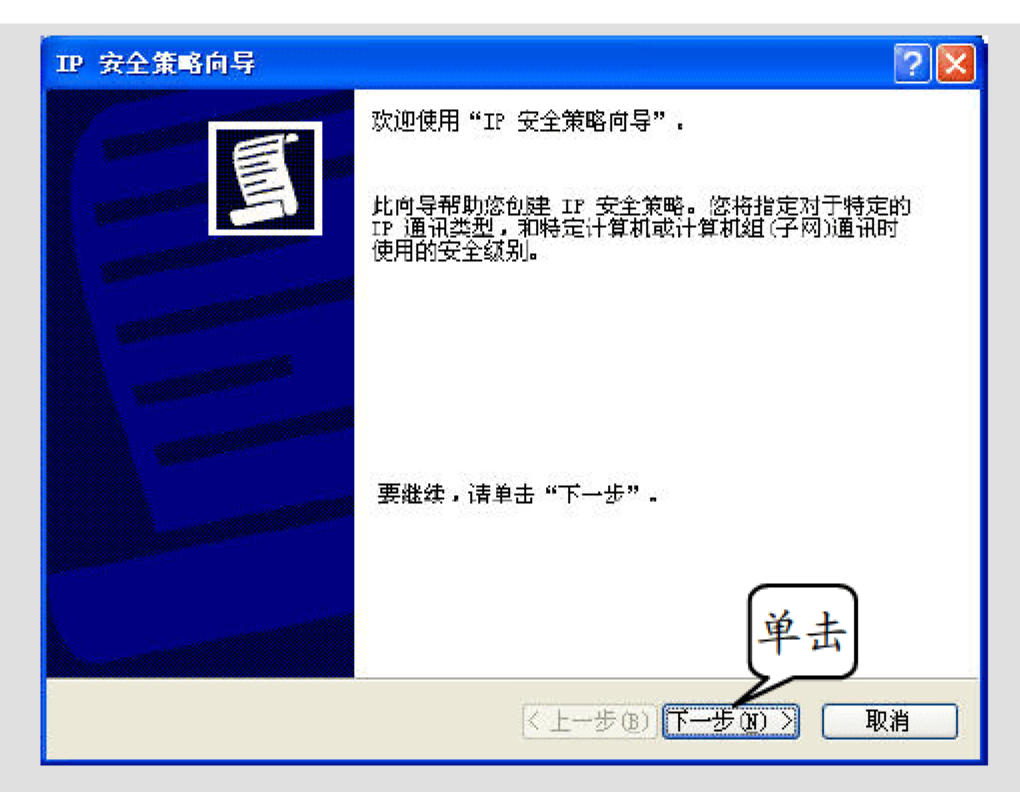


图 4-52　【IP 安全策略向导】对话框

（3）在【IP 安全策略名称】对话框的【名称】文本框中输入策略名称，如“端口策略”，单击【下一步】按钮，如图 4-53 所示。

（4）在【安全通讯请求】对话框中，禁用【激活默认响应规则】复选框，并单击【下一步】按钮，如图 4-54 所示。



图 4-53　【IP 安全策略名称】对话框

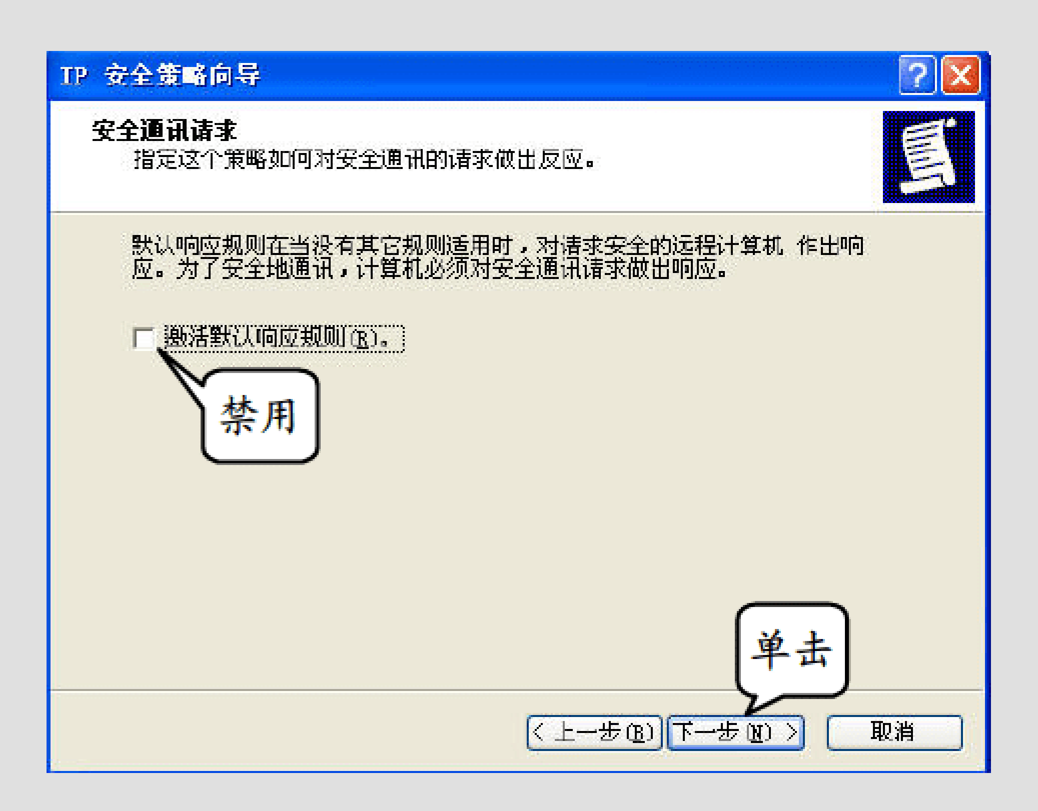


图 4-54　【安全通讯请求】对话框

（5）在【IP 安全策略向导】对话框中，单击【完成】按钮，如图 4-55 所示。

（6）在弹出的【端口策略 属性】对话框的【规则】选项卡中，禁用【使用“添加向导”】复选框，并单击【添加】按钮，如图 4-56 所示。

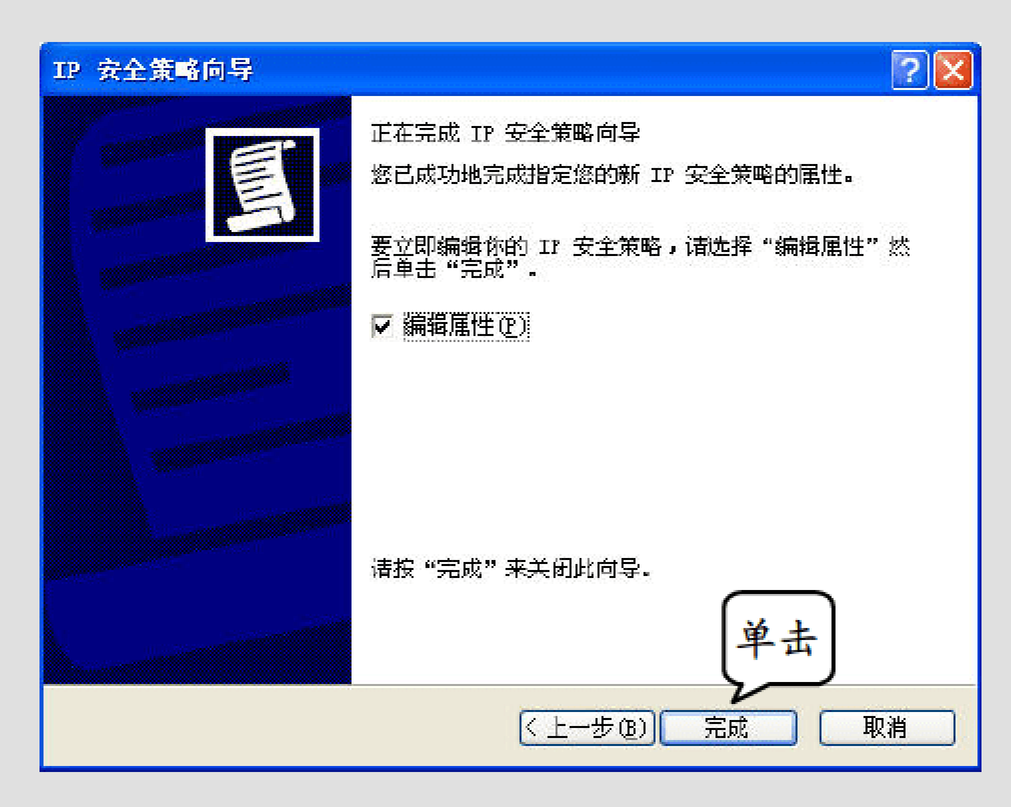


图 4-55　【IP 安全策略向导】对话框



图 4-56　端口【规则】选项卡

（7）在弹出的【新规则 属性】对话框的【IP 筛选器列表】选项卡中，单击【添加】按钮，如图 4-57 所示。

（8）在弹出的【IP 筛选器列表】对话框的【名称】文本框中输入名称，如“端口规则”，禁用【使用“添加向导”】复选框，然后单击【添加】按钮，如图 4-58 所示。

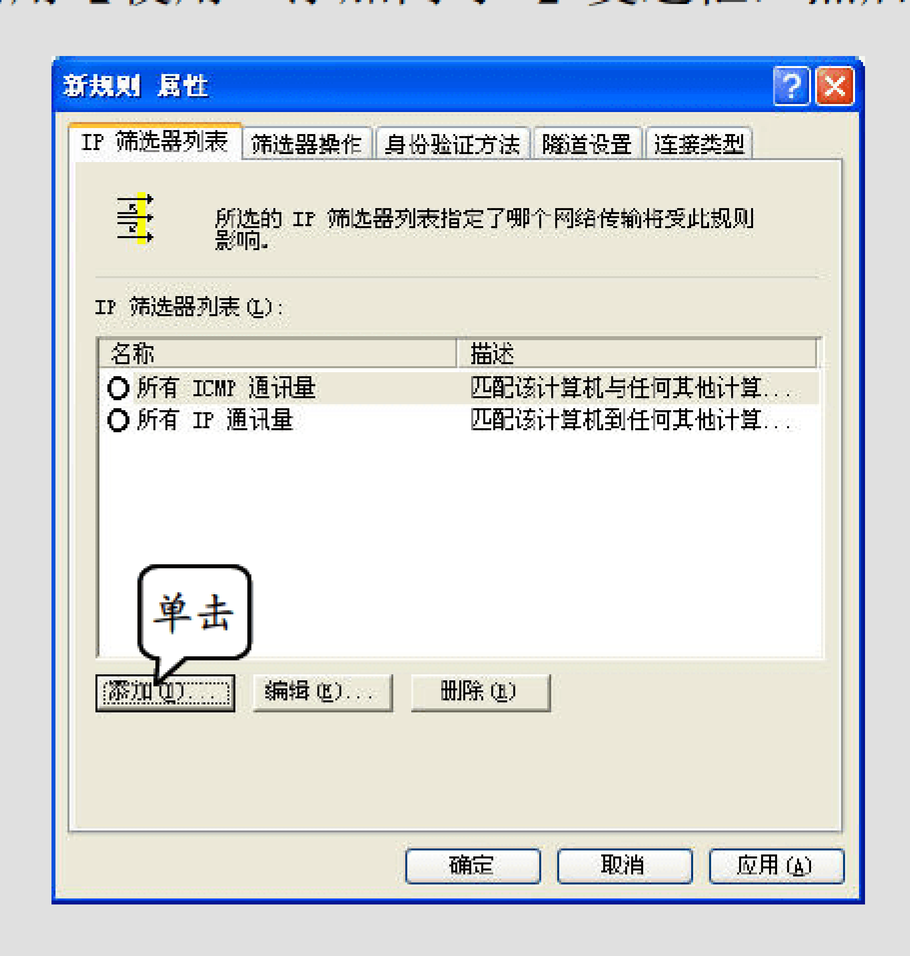


图 4-57 【新规则 属性】对话框

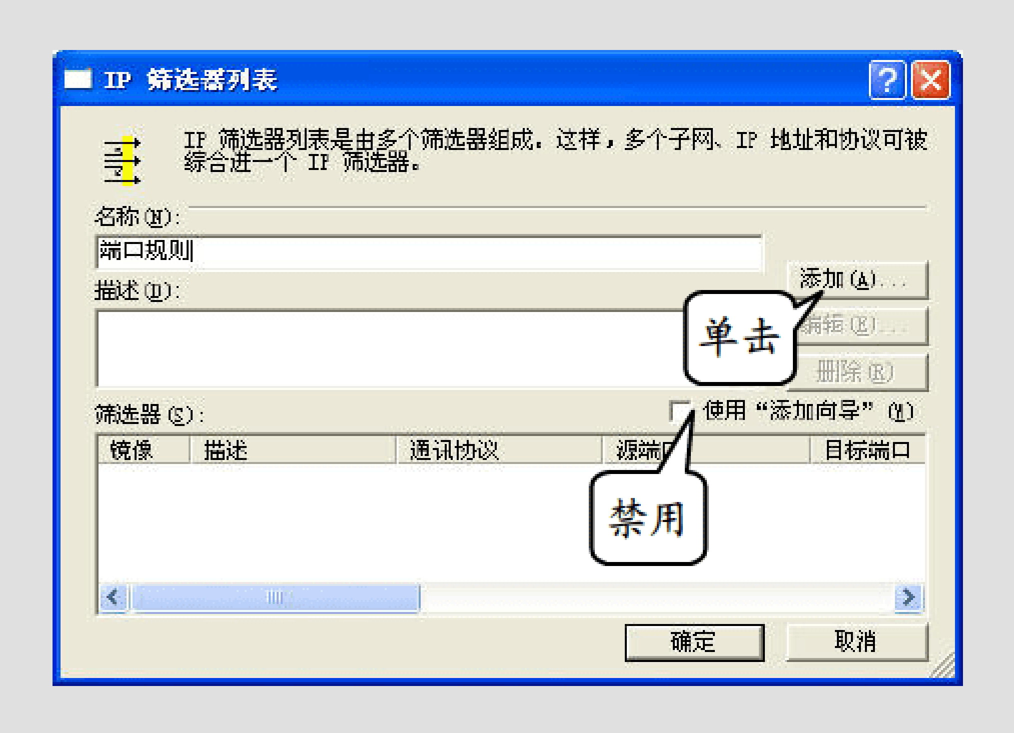


图 4-58 【IP 筛选器列表】对话框

（9）在弹出的【筛选器 属性】对话框的【寻址】选项卡中，选择【源地址】下拉列表框为【任何 IP 地址】选项，选择【目标地址】下拉列表框为“我的 IP 地址”，如图 4-59 所示。

（10）在该对话框的【协议】选项卡中，选择【选择协议类型】下拉列表框为 TCP 选项，如图 4-60 所示。

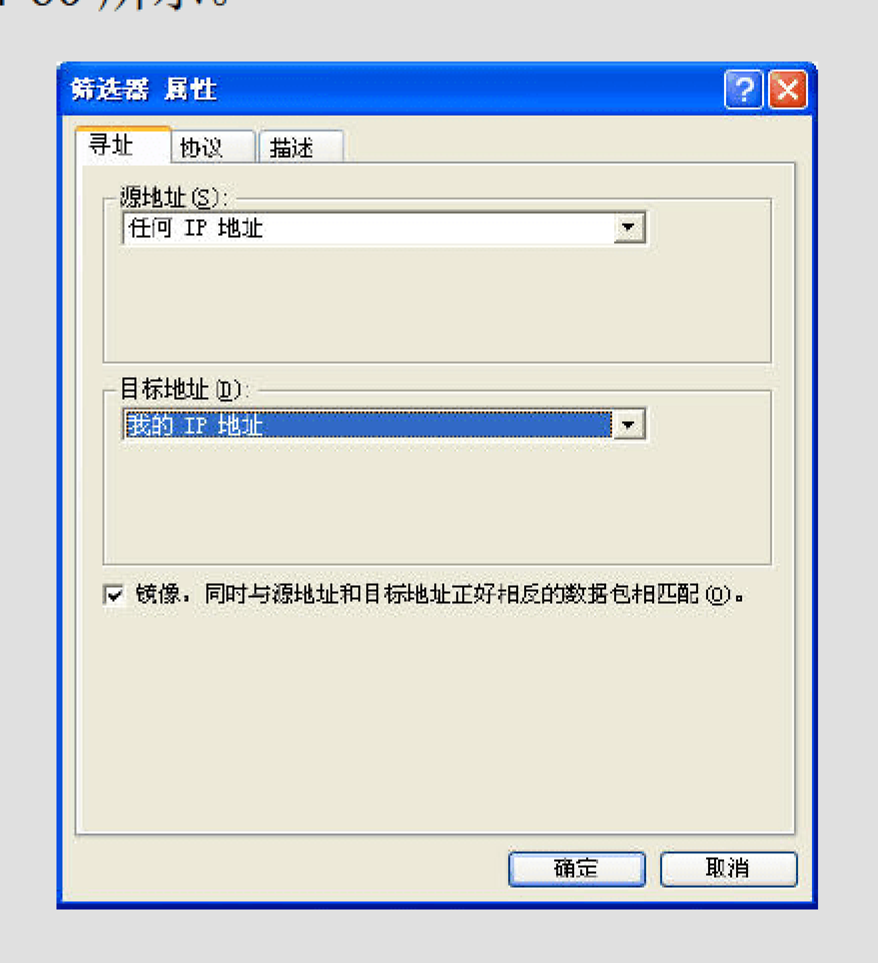


图 4-59 【筛选器 属性】对话框

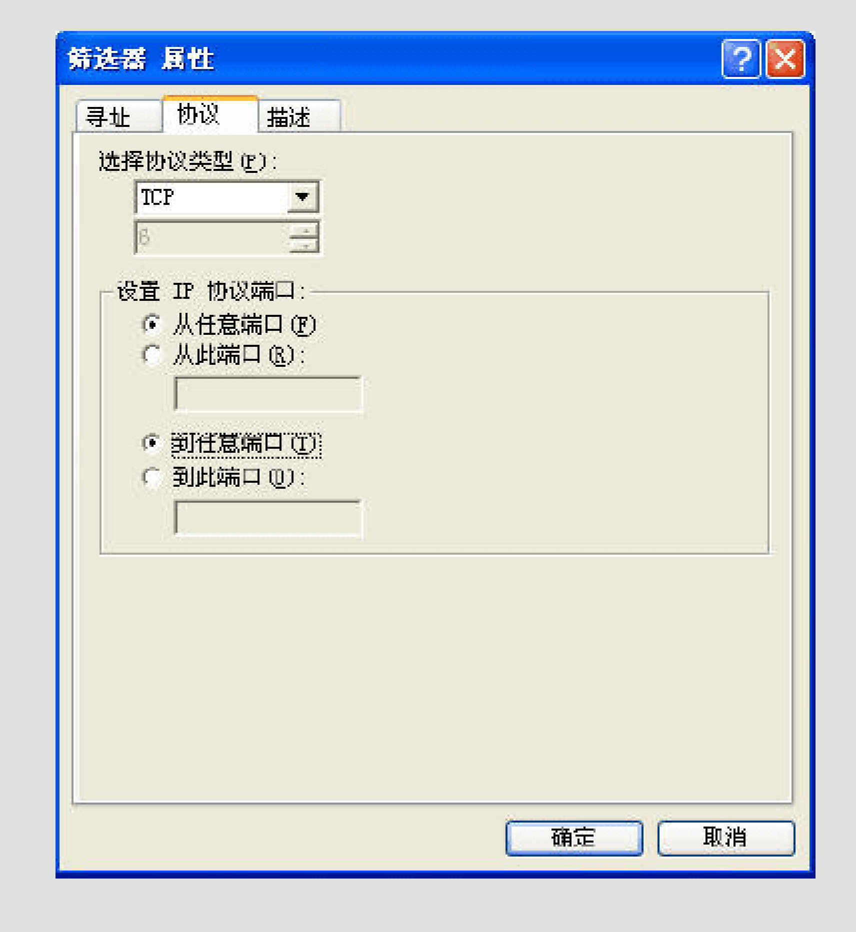
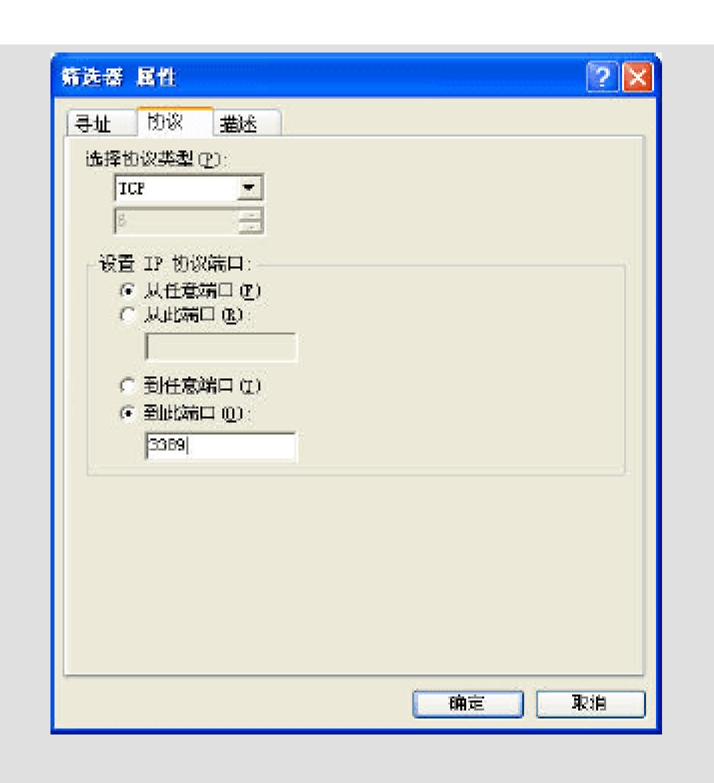


图 4-60 【筛选器 属性】对话框

（11）在【设置 IP 协议端口】栏中，选中【从任意端口】和【到此端口】单选按钮，并在【到此端口】文本框中输入“3389”，然后单击【确定】按钮，如图 4-61 所示。

（12）在【IP 筛选器列表】对话框中，单击【确定】按钮，如图 4-62 所示。

（13）在【新规则 属性】对话框中，选中【端口规则】单选按钮，并选择【筛选器操作】选项卡，如图 4-63 所示。



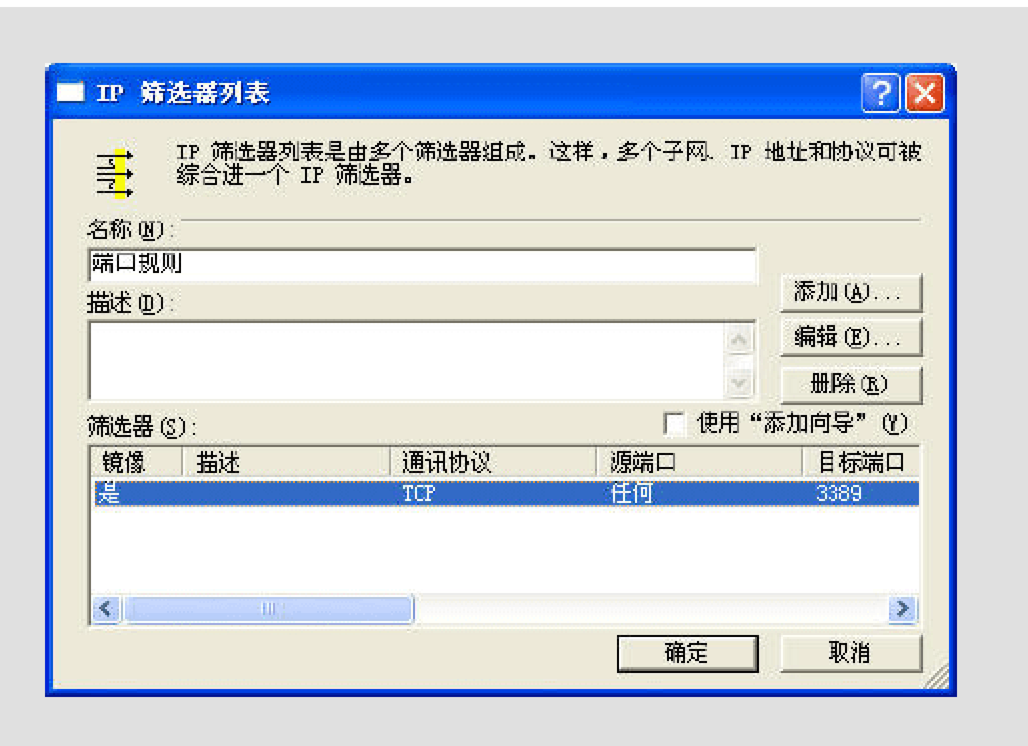
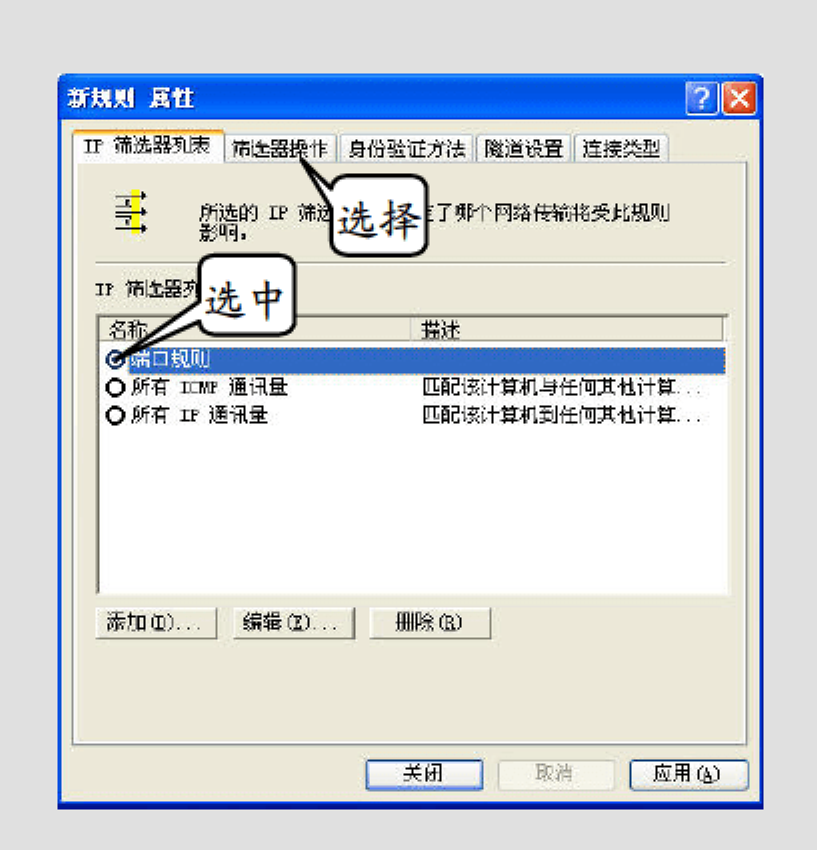


图 4-61 【协议】选项卡　　图 4-62 【IP 筛选器列表】对话框

（14）在【筛选器操作】选项卡中，禁用【使用“添加向导”】复选框，并单击【添加】按钮，如图 4-64 所示。



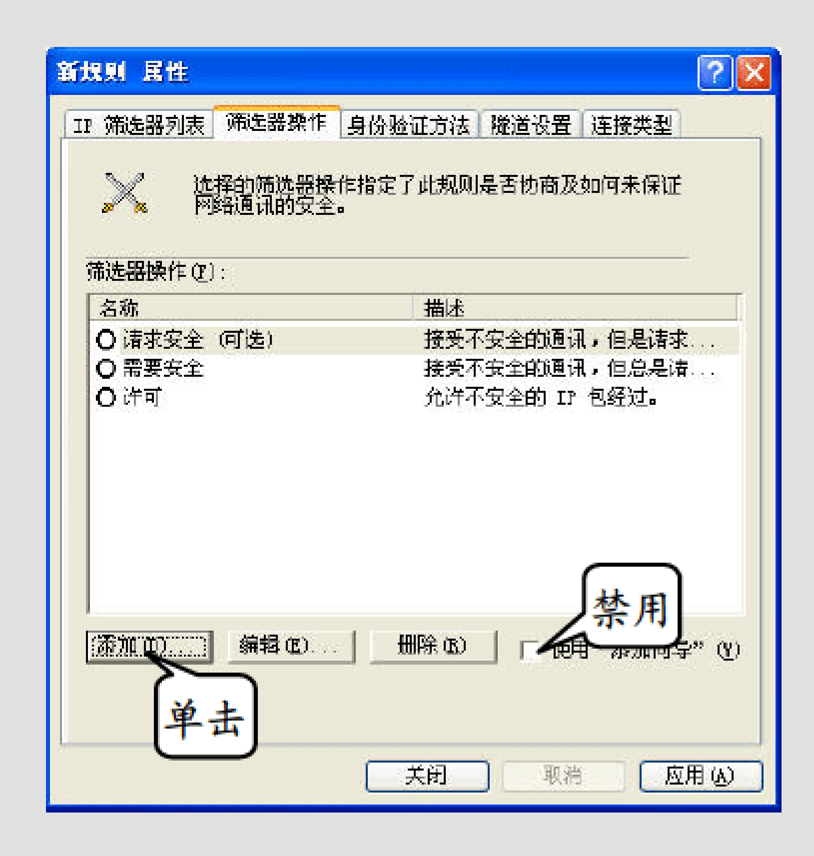
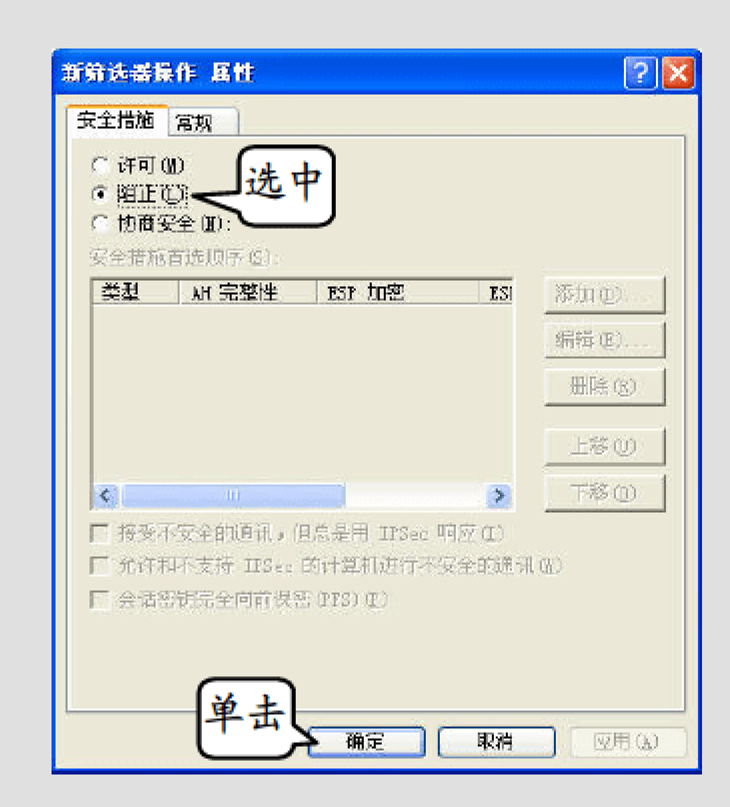


图 4-63 IP 筛选器列表　　图 4-64 【筛选器操作】选项卡

（15）在弹出的【新筛选器操作 属性】对话框的【安全措施】选项卡中，选中【阻止】单选按钮，单击【确定】按钮，如图 4-65 所示。

（16）在【新规则 属性】对话框的【筛选器操作】选项卡中，选中【新筛选器操作】单选按钮，并单击【关闭】按钮，如图 4-66 所示。



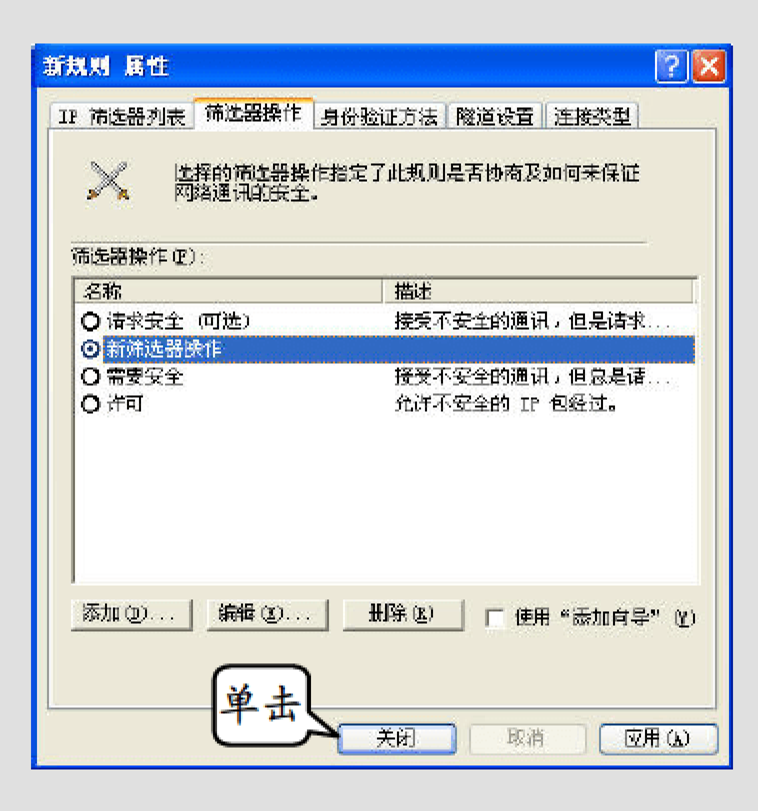
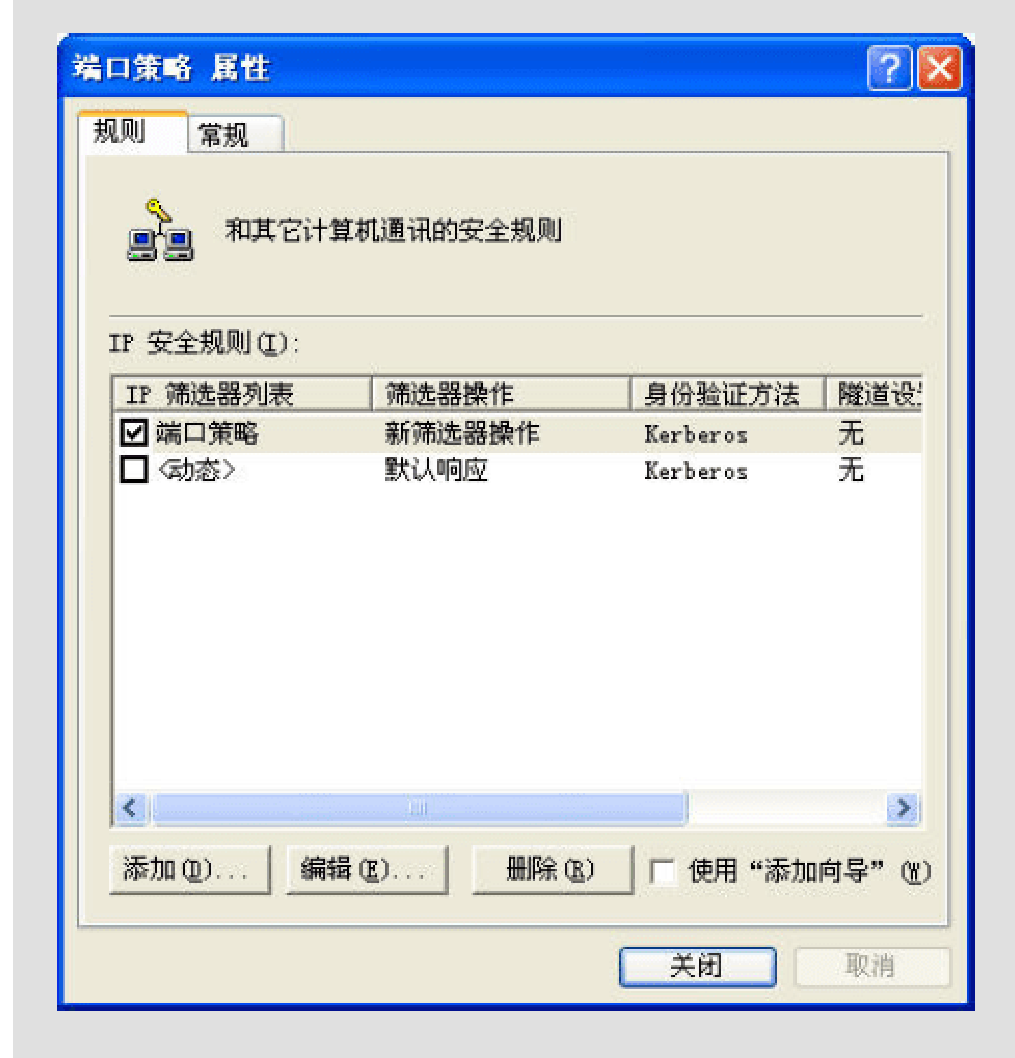


图 4-65 【新筛选器操作 属性】对话框　　图 4-66 【新规则 属性】对话框

（17）在【端口策略 属性】对话框中，单击【关闭】按钮，如图 4-67 所示。

（18）在【本地安全设置】窗口中，双击【IP 安全策略，在本地计算机】选项，并右击右侧窗格中的【端口策略】选项，执行【指派】命令，如图 4-68 所示。



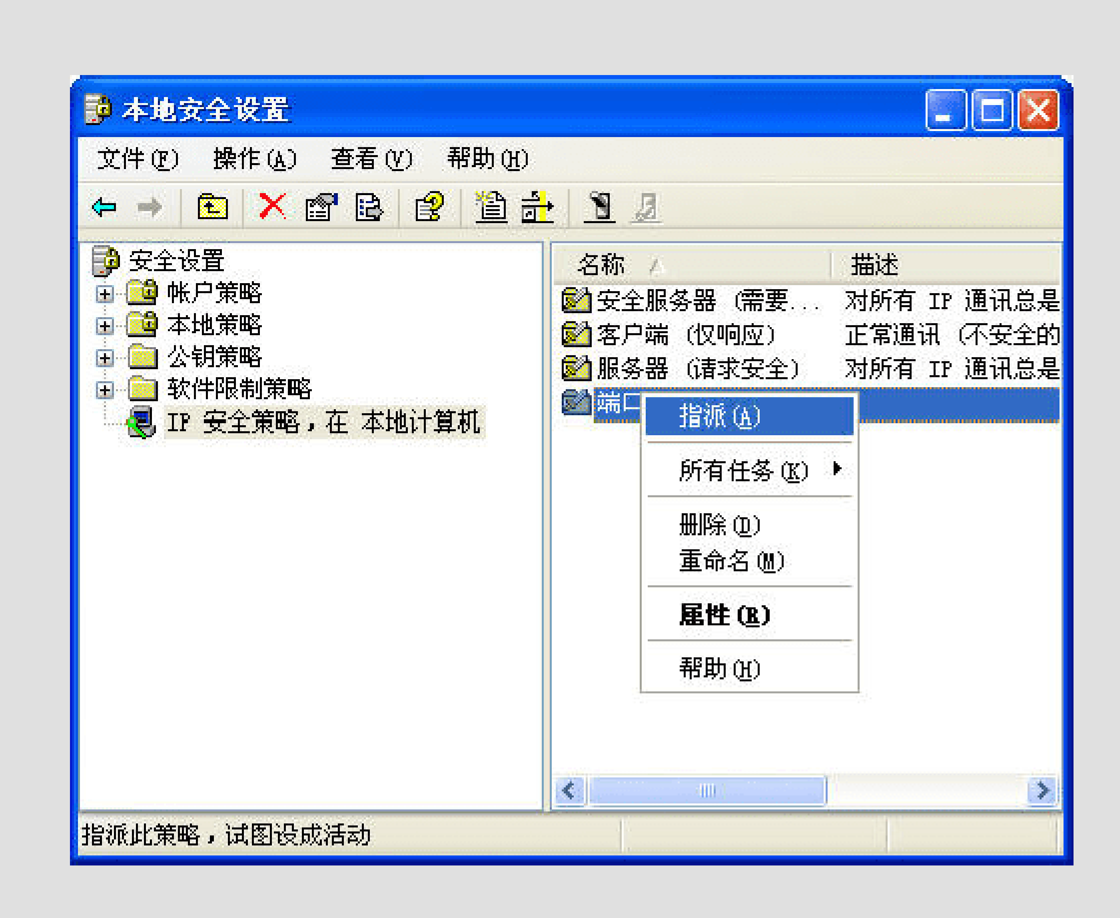




图 4-67 【端口策略 属性】对话框

图 4-68 【本地安全设置】窗口

（19）重新启动计算机，使本地安全策略生效即可。

4.5.2 操作实例——查看端口

Tcpview 工具可以动态查看本机开放了哪些端口，正在与哪一个远程端口连接，以及当前端口状态。

1. 实例目的

- 查看本机当前端口。
- 查看远程服务端口。
- 查看端口状态。

2. 实例步骤

（1）在桌面双击【Tcpview 汉化版】应用程序图标，如图 4-69 所示。

（2）在 TCPView-Sysinternals:www.sysinternals.com 窗口的菜单栏中，单击【选项】菜单，并执行【字体】命令，如图 4-70 所示。

（3）在【TCPView 字体】对话框中的【大小】下拉列表内，选择“9”选项，然后单击【确定】按钮，如图 4-71 所示。

（4）在 TCPView-Sysinternals:www.sysinternals.com 窗口中，可查看到“通信协议”、“本地地址”、“远程地址”等信息，如图 4-72 所示。



图 4-69　Tcpview 应用程序图标

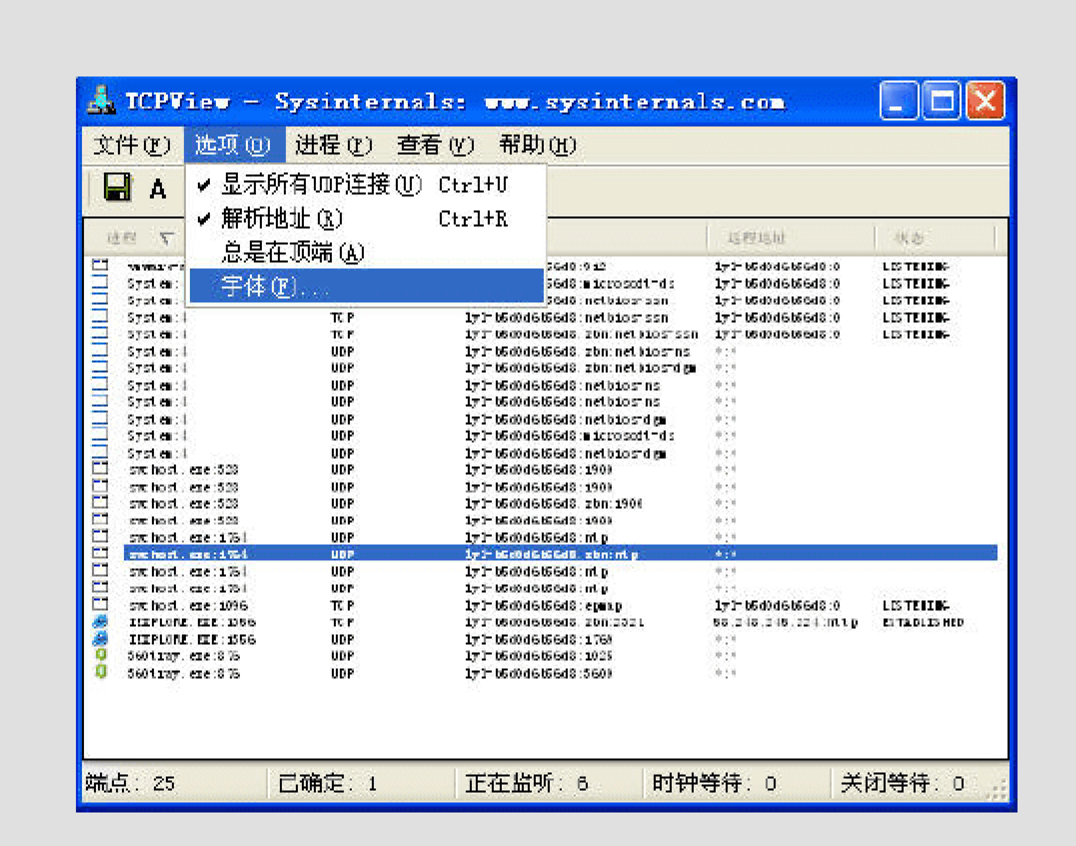


图 4-70　执行【字体】命令

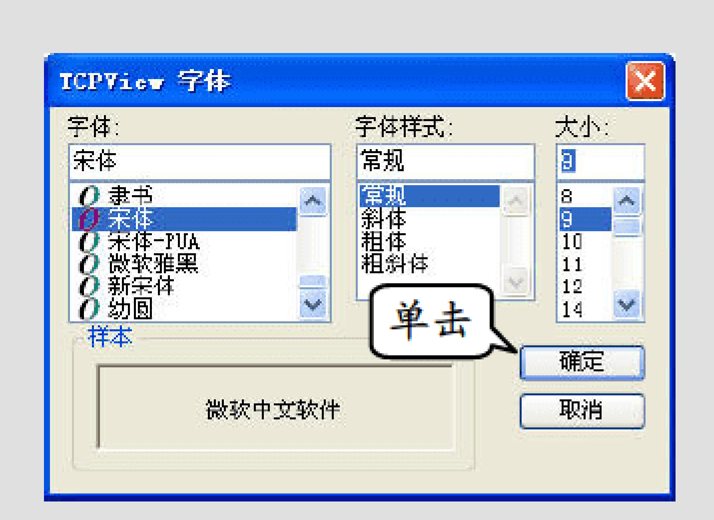


图 4-71　调整字体大小

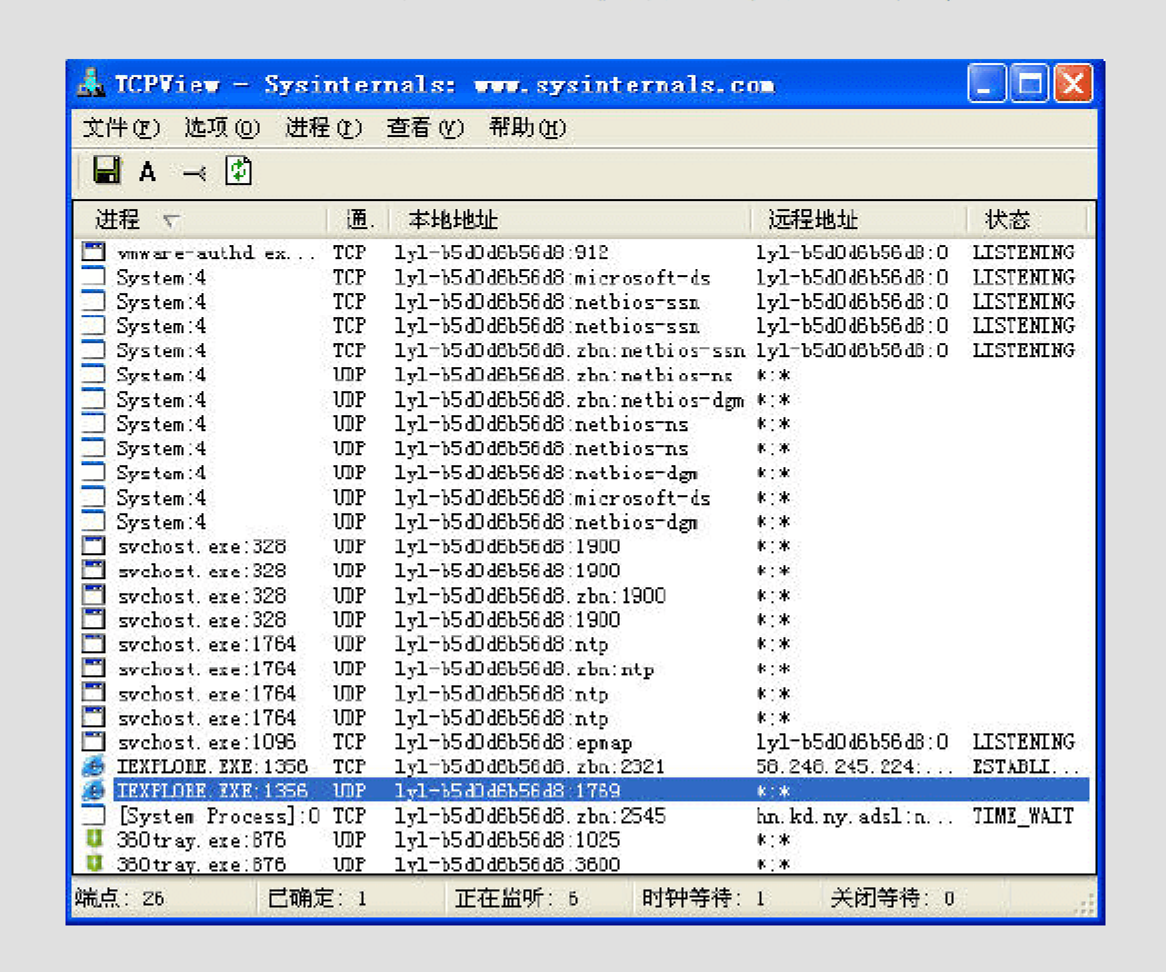


图 4-72　查看详细信息



Tcpview 第一次运行时，字体很小，需要较大字体时，只需调整字体大小即可。

4.5.3　操作实例——使用 TCP/IP 筛选器

TCP/IP 筛选器是一个 Windows 自带的功能简单的防火墙，能够筛选入站数据，保证计算机安全。

1. 实例目的

- ❑ 屏蔽不安全的进站流量。
- ❑ 阻止端口入站数据。
- ❑ 提高系统安全性能。

2. 实例步骤

（1）执行【开始】|【运行】命令，在【打开】文本框中，输入ftp://192.168.0.9命令，并单击【确定】按钮，进入 ftp://192.168.0.9 窗口，如图 4-73 所示。

（2）在桌面执行【开始】|【设置】|【控制面板】命令，如图 4-74 所示。




图 4-73　ftp 窗口

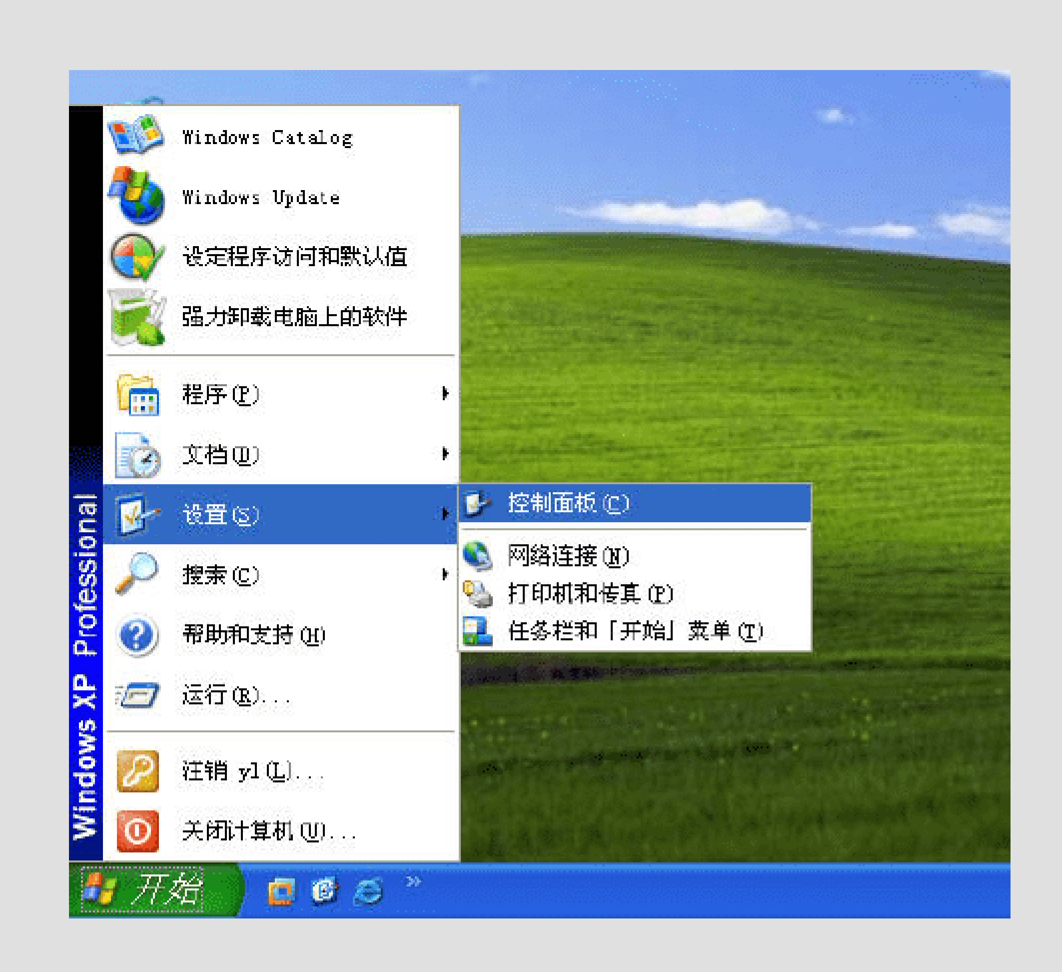


图 4-74　执行【控制面板】命令

（3）在【控制面板】窗口中，双击【网络连接】图标，如图 4-75 所示。

（4）在【网络连接】窗口中，右击【本地连接】图标，并执行【属性】命令，如图 4-76 所示。

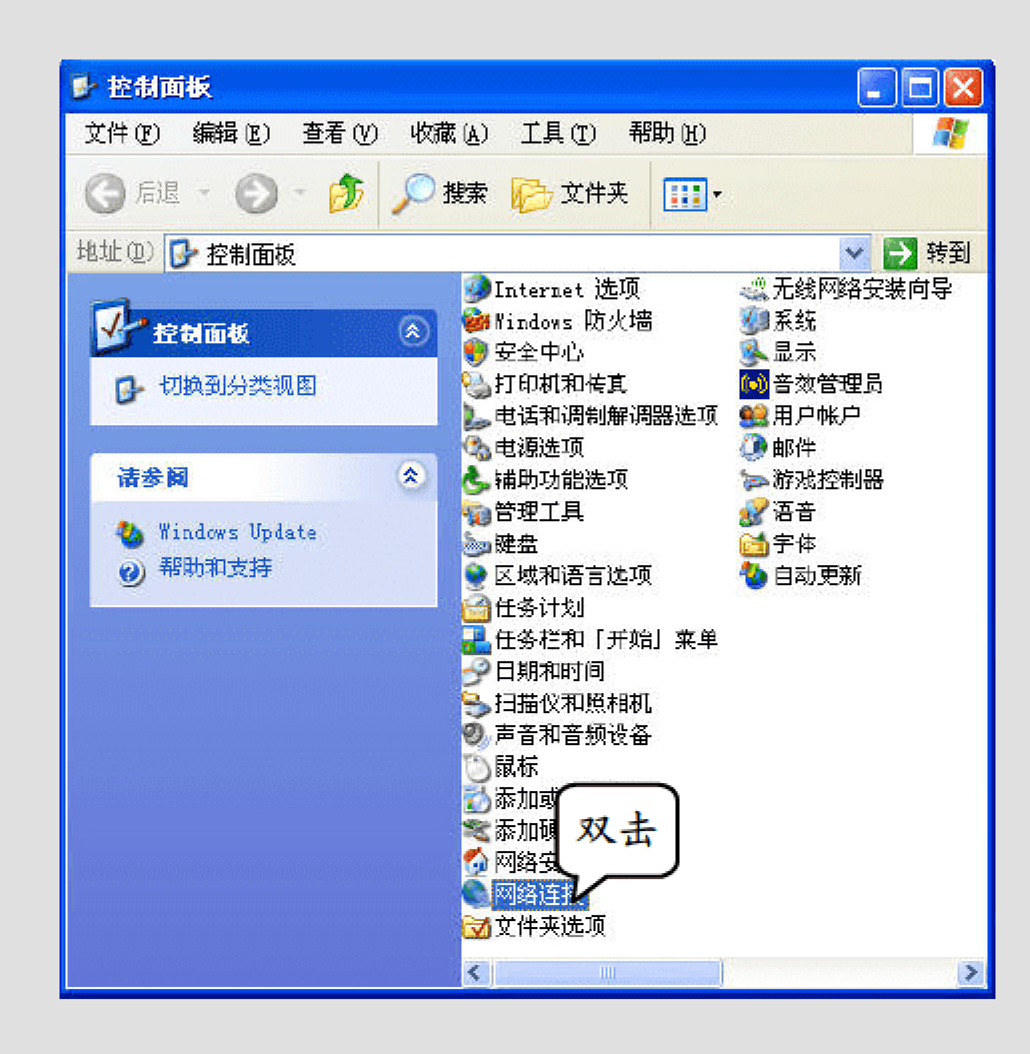


图 4-75　【控制面板】窗口

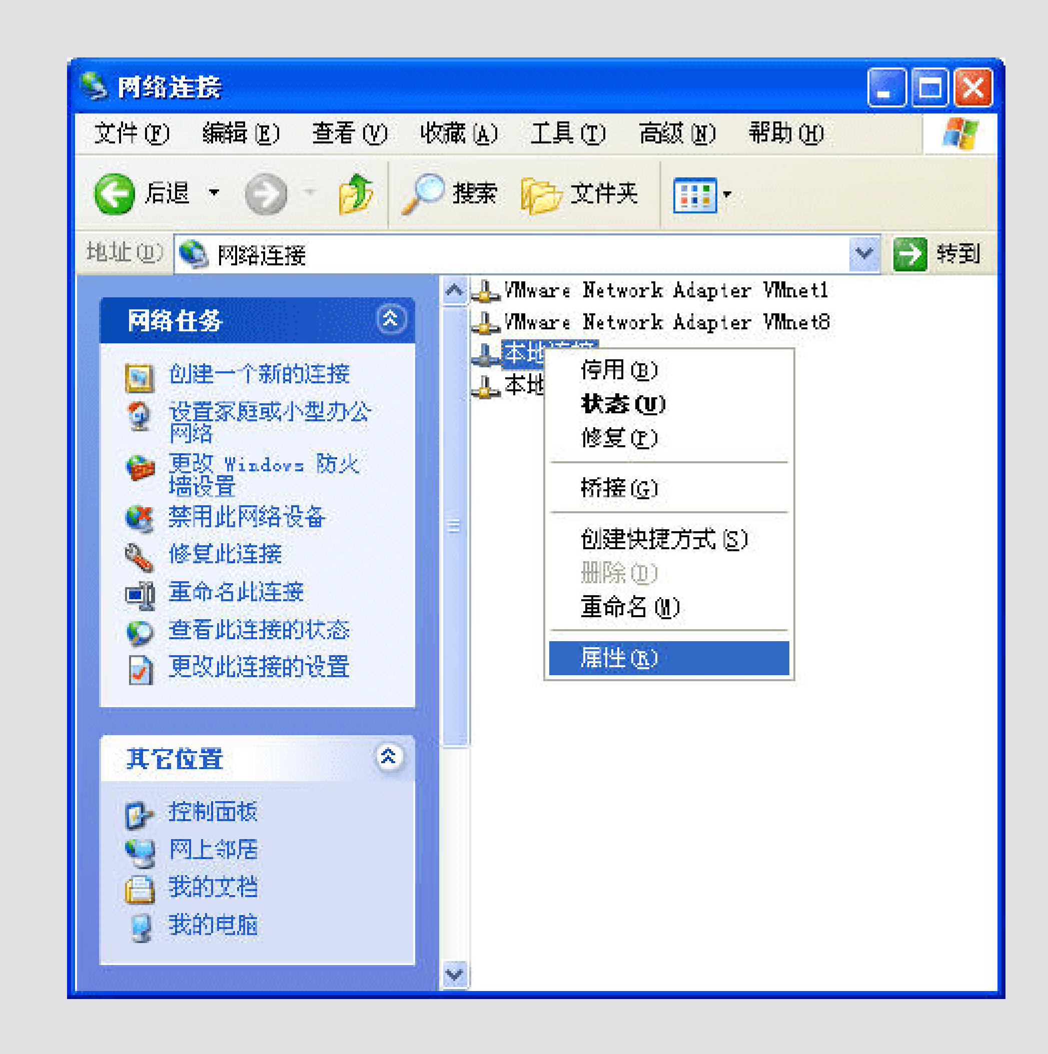


图 4-76　【网络连接】窗口

（5）在弹出的【本地连接 属性】对话框的【常规】选项卡中，双击【Internet 协议（TCP/IP）】

选项，如图 4-77 所示。

（6）在弹出的【Internet 协议 （TCP/IP） 属性】对话框中，单击【高级】按钮，如图 4-78 所示。

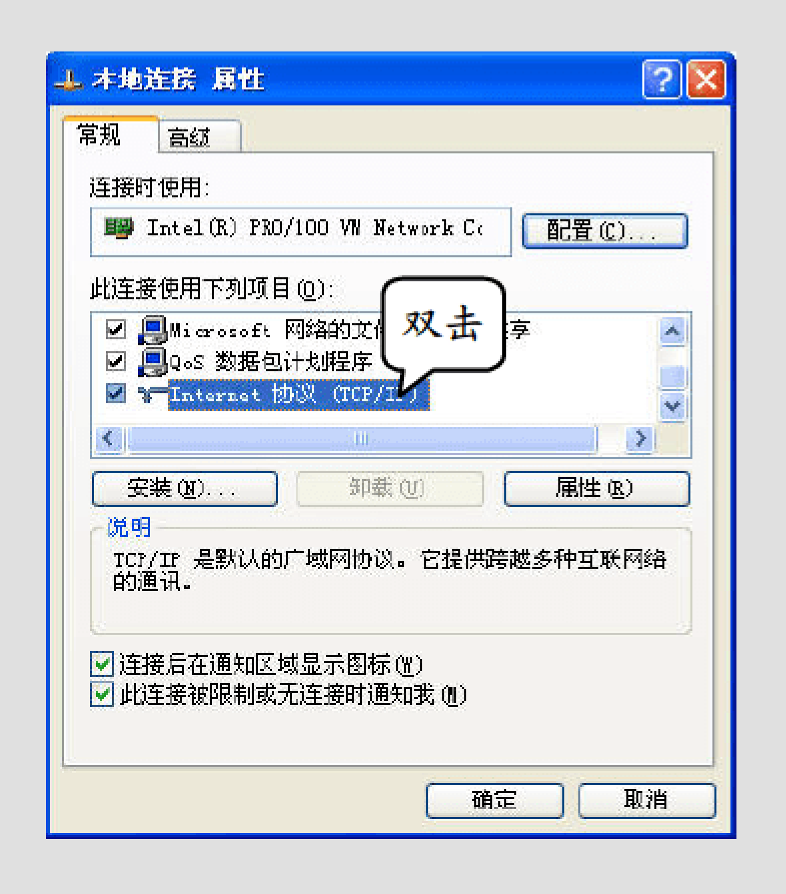


图 4-77 【本地连接 属性】对话框

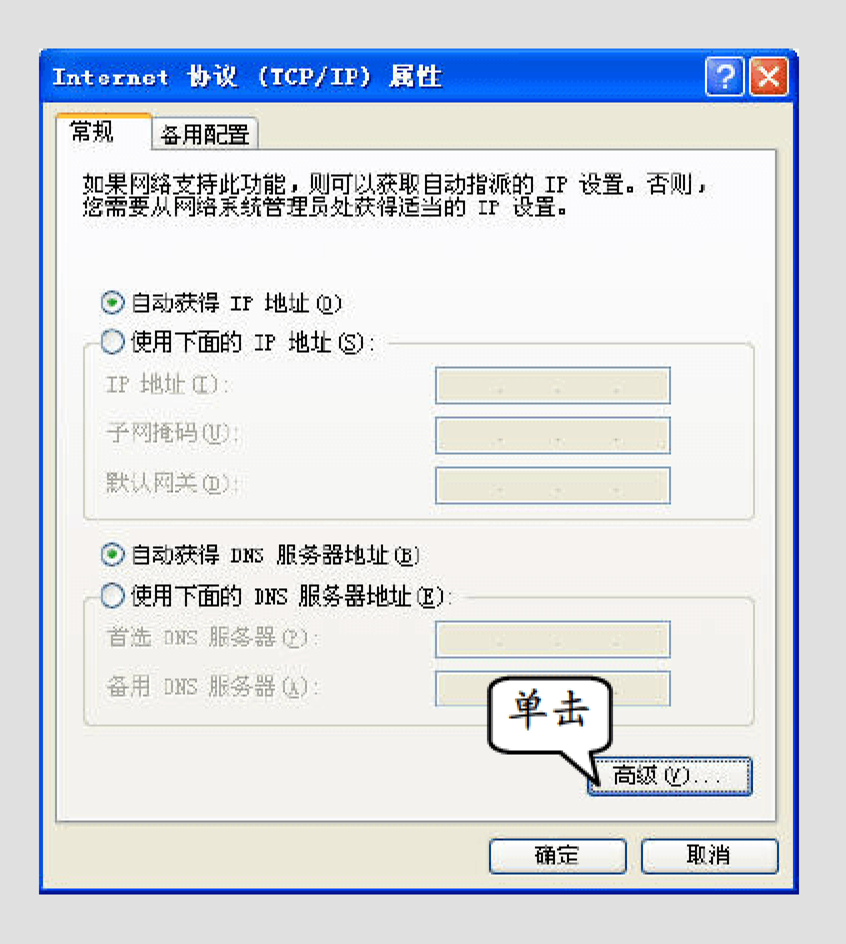


图 4-78 【常规】选项卡

（7）在弹出的【高级 TCP/IP 设置】对话框中，选择【选项】选项卡，如图 4-79 所示。

（8）在【选项】选项卡中，单击【属性】按钮，如图 4-80 所示。

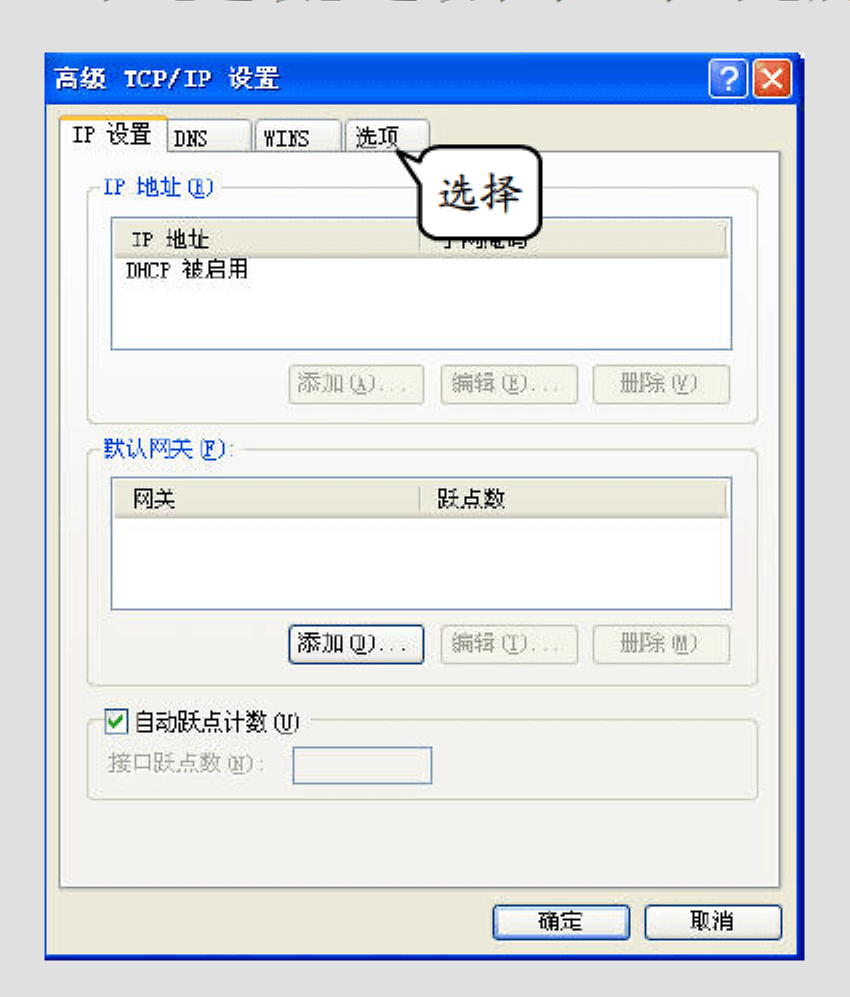


图 4-79 【高级 TCP/IP 设置】对话框



图 4-80 【高级 TCP/IP 设置】对话框

（9）在【TCP/IP 筛选】对话框中，启用【启用 TCP/IP 筛选（所有适配器）】复选框，并选中【只允许】单选按钮，然后单击【确定】按钮，如图 4-81 所示。

（10）返回到【本地连接 属性】对话框中，单击【确定】按钮，如图 4-82 所示。

（11）在弹出的【本地网络】对话框中，单击【是】按钮，如图 4-83 所示。

（12）在桌面执行【开始】|【运行】命令，然后在【打开】文本框中输入ftp://192.168.0.9 命令，并单击【确定】按钮，查看访问结果，如图 4-84 所示。

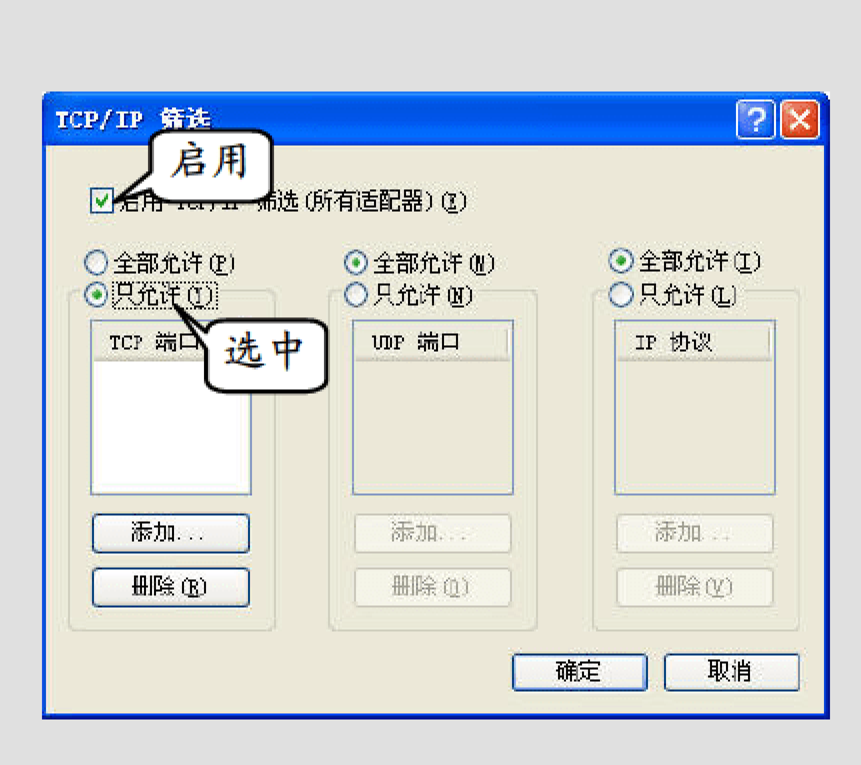


图 4-81 【TCP/IP 筛选】对话框

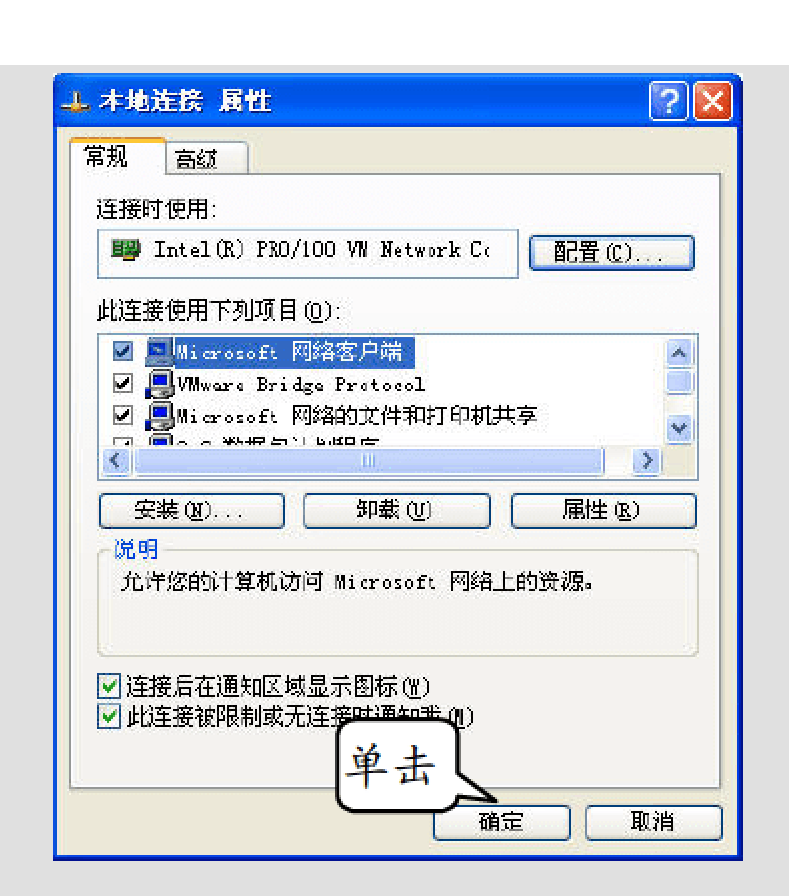


图 4-82 【本地连接 属性】对话框

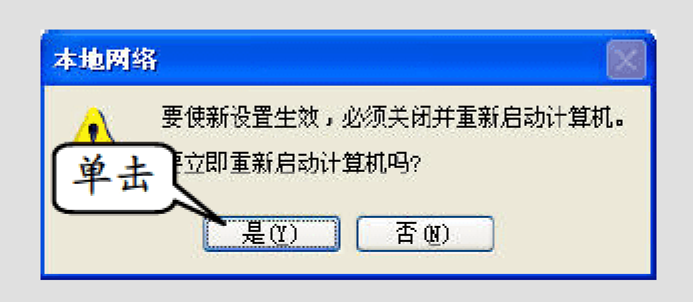


图 4-83 【本地网络】对话框

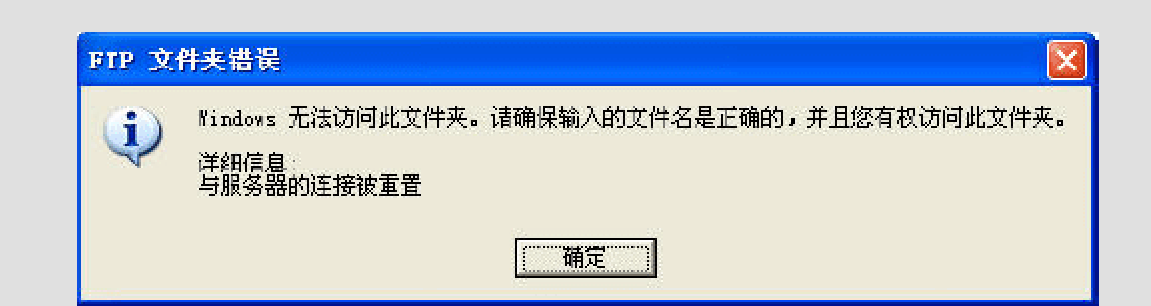


图 4-84 【FTP 文件夹错误】对话框

第5章 系统安全策略

在服务器操作系统中，安全策略是影响服务器安全性的主要设置之一。而所有的安全策略都是基于计算机配置的策略。为了保证网络和系统的安全性，管理员可以根据不同用户对网络的访问需求，建立相应的组织单位（OU），再对定制的组织单位统一部署安全策略，这对用户端数量的影响取决于组织单位中用户的多少。

在 Windows Server 2008 中，提供了强大的安全机制，但在默认状态下并没有配置。因此，需要管理员根据实际网络环境进行配置。本章从账户策略、审核策略及限制用户登录、安全配置和分析等方面进行介绍，使用户充分了解并掌握系统安全策略。

本章学习要点：

- 熟悉账户策略和审核策略
- 了解用户权限及掌握限制用户登录的方法
- 了解安全配置和分析
- 熟悉企业系统监控安全策略
- 掌握 IPSec 安全策略

5.1 账户策略

目前，企业或单位用户账户的保护主要通过采用密码保护机制来实现，为了避免用户身份因密码被破解而被他人夺取或盗用内部资源现象的发生，通常可采取提高密码的破解难度、启用账户锁定策略、限制用户登录、限制外部连接和防范网络嗅探等措施。

所有的安全策略都是基于计算机配置的策略。账户策略定义在计算机上，然而可以影响用户与计算机或域交互作用的方式。账户策略由密码策略和账户锁定策略两部分组成。

5.1.1 密码策略

密码是用户登录系统和网络的唯一凭证，如果密码丢失也就无法登录。另一方面，被他人获取密码会给计算机或网络带来安全隐患。

密码策略主要用于域或本地用户账户。提高密码的破解难度主要是通过提高密码复杂性、增加密码长度、增加更换频率等措施来实现，但这对于普通用户来讲很难做到，因此，对于企业网络中的一些敏感用户就必须采取一些相关措施，以强制性方式来改变那些不安全的

密码。

在 Windows Server 2008 中，系统默认已经启用了用户账户密码策略，通过执行【开始】|【管理工具】|【本地安全策略】命令，在打开的窗口中，展开【账户策略】节点，并选择【密码策略】选项，即可查看到所有的密码策略，如图 5-1 所示。

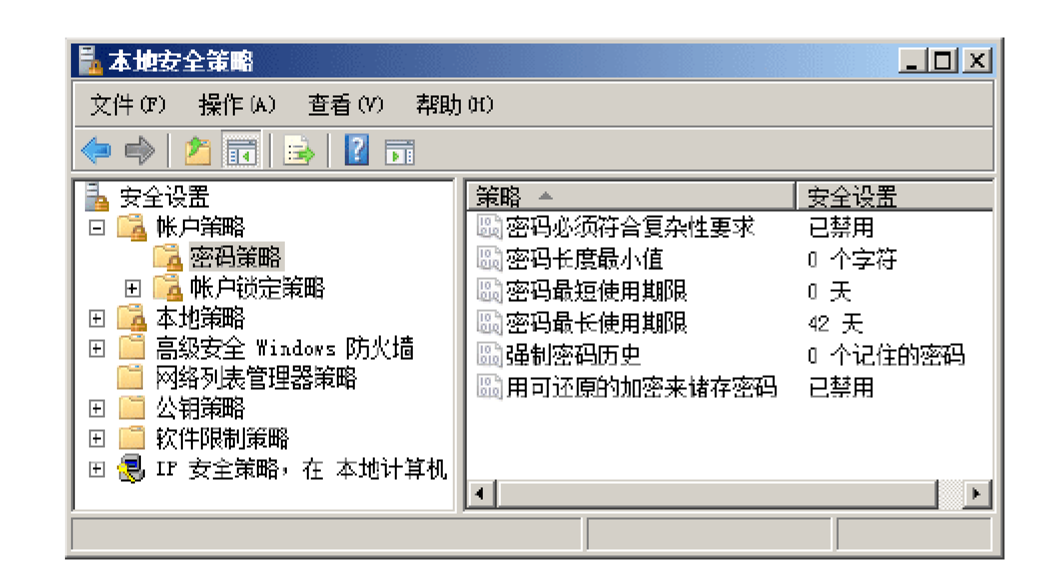


图 5-1　【本地安全策略】窗口

1. 密码必须符合复杂性要求

该策略用于强制用户必须使用经过复杂设置的密码，通常要求密码必须满足以下条件。

- ❑ 不包含全部或部分的用户账户名。
- ❑ 密码长度至少为 8 个字符，且包含表 5-1 所示的 4 种类别的字符。
- ❑ 更改或创建密码时，会强制执行复杂密码需求检测。

表 5-1　可用密码字符

类别	字符范围
英文大写字母	A～Z
英文小写字母	a～z
基本数字	0～9
非字母字符	!、$、#、%

如果要设置该策略，只需在【本地安全策略】窗口中的【密码策略】列表中，双击【密码必须符合复杂性要求】选项，在弹出的对话框中，选中【已启用】单选按钮，并单击【确定】按钮，如图 5-2 所示。

2. 密码长度最小值

该安全策略用于确定用户账户的密码可以包含的最少字符数。可以设置为 1～14 个字符间的某个值，或者设置为 0，若设置为 0，则表明不需要密码。

如果需要设置该策略，需要在【本地安全策略】窗口中的【密码策略】列表中，双击【密码必须符合复杂性要求】选项，在弹出对话框的【不要求密码】文本框中，设置密码长度的最小值，图 5-3 所示为系统默认设置。然后，单击【确定】按钮。

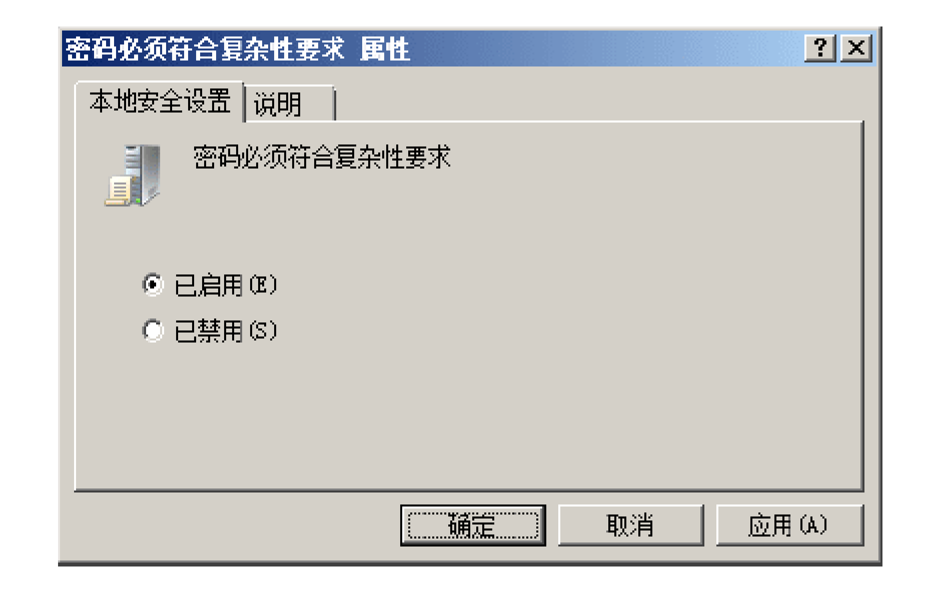
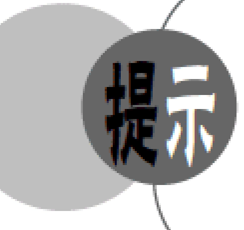


图 5-2　设置密码必须符合复杂性要求策略



图 5-3　设置密码长度最小值



在企业网络中，通常建议将敏感用户的密码长度设置在 16 位以上。这对于用户来讲，在登录网络的时候比较烦琐，但是对于黑客来讲却提高了密码破解的难度，同时配合密码复杂度策略，将提高网络的安全性。

3．密码最长使用期限

该策略要求用户在更改密码之前可以使用该密码的时间（以天为单位）。可以将密码的过期天数设置在 1～999 天之间，或将其设置为 0（表示密码永不过期）。

另外，如果密码最长使用期限设置在 1～999 天之间，那么密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0，则密码最短使用期限可以是 0～998 之间的任意数字。

如果要设置该策略，需要在【本地安全策略】窗口中的【密码策略】列表中，双击【密码最长使用期限】选项，并在弹出对话框的【密码过期时间】文本框中，输入过期天数，如 60。然后，单击【确定】按钮，如图 5-4 所示。



图 5-4　设置密码最长使用期限



使用该策略，攻击者只能在有限的时间内破解用户密码并访问网络的资源。建议将网络中敏感用户密码的最长使用期限设置为 7 天。

4．密码最短使用期限

该安全策略用于确定用户在更改密码之前必须使用该密码的时间（以天为单位）。可以设置为 1～998 之间的某个值，或将其设置为 0，即允许立即更改密码。

密码最短使用期限必须小于密码最长使用期限，除非密码最长使用期限设置为 0（表明密码永不过期）。如果密码最长使用期限设置为 0，那么密码最短使用期限可以设置为 0～998 天之间的任意值。

另外，如果希望强制密码历史有效，需要将密码最短有效期限设置为大于 0。如果没有密码最短有效期限，则用户可以重复循环通过密码，直到获得喜欢的旧密码。如果将该密码的历史记录设置为 0，则用户不必选择新密码。因此，默认情况下将密码历史记录设置为 1。

如果要设置该策略，需要在【本地安全策略】窗口中的【密码策略】列表中，双击【密码最短使用期限】选项，并在弹出对话框中设置密码最短使用期限，图 5-5 所示为系统默认设置为 0 天，单击【确定】按钮。

5．强制密码历史

该策略能够确保旧密码不能再继续使用，从而增加系统或网络的安全性。在重新使用旧密码之前，该安全策略确定与某个用户账户相关的唯一新密码的数量，这个值必须是 0～24

之间的某一个数值，推荐值为8，这样既便于用户记忆，又很难被他人猜测到。

如果要设置该策略，需要在【本地安全策略】窗口中的【密码策略】列表中，双击【强制密码历史】选项，并在弹出对话框的【保留密码历史】文本框中，输入保留天数，如8。然后，单击【确定】按钮，如图5-6所示。

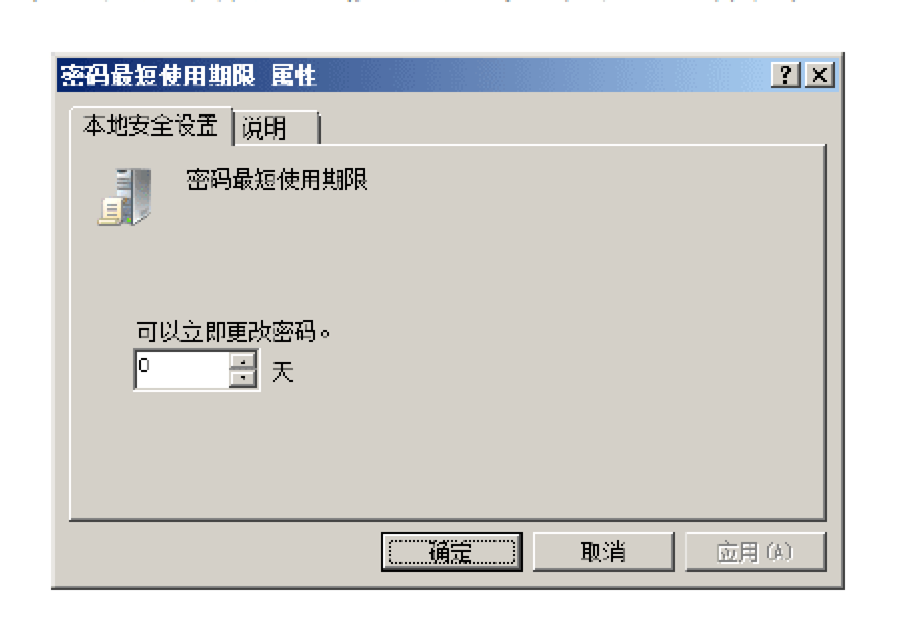


图5-5　设置密码最短使用期限



图5-6　设置密码保留天数



经科学研究表明，人能够瞬间记忆的数字最大值为8位。因此，选择采用8个字符作为密码可以兼顾记忆和安全两个方面。

6. 用可还原的加密来存储密码

该安全策略能够确定操作系统是否使用可还原的加密来存储密码。如果应用程序使用了要求知道用户密码才能进行身份验证的协议，则该策略可对它提供支持。可还原的加密存储密码和存储明文版本密码本质上是相同的。因此，除非应用程序有比保护密码信息更重要的要求，否则不必使用该策略。

另外，当使用质询握手身份验证协议（CHAP）通过远程访问或Internet身份验证服务（IAS）进行身份验证时，必须使用该策略。在Internet信息服务（IIS）中使用摘要式验证时也要求使用该策略。

如果要设置该策略，需要在【本地安全策略】窗口中的【密码策略】列表中，双击【用可还原的加密来存储密码】选项，在弹出的对话框中，选中【已启用】单选按钮，并单击【确定】按钮，如图5-7所示。

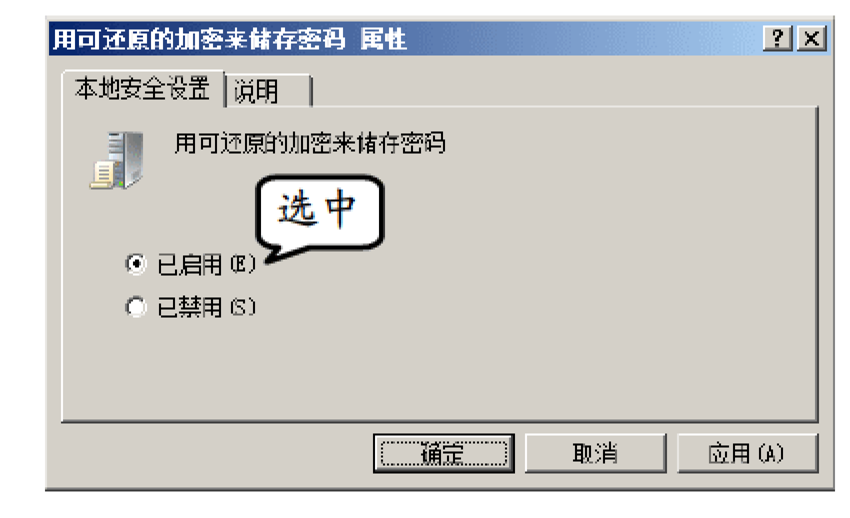


图5-7　用可还原的加密来存储密码

5.1.2　账户锁定策略

账户锁定是指在某些情况下，如果账户受到密码词典或暴力破解等方式的在线自动登录工具的攻击，为了保护该账户的安全而将此账户进行锁定，使其在一段时间内不能再次被使用的策略，这样就可以挫败那些连续的尝试猜解行为。

在Windows Server 2008中，系统默认并没有对这些策略进行设置。通过执行【开始】|【管理工具】|【本地安全策略】命令，在打开的窗口中，展开【账户策略】节点，并选择【账

户锁定策略】选项，即可查看到所有的策略，如图 5-8 所示。因此，对于恶意的攻击也没有任何限制。只要攻击者有足够的耐心，那么通过自动登录工具和密码猜解字典进行攻击，甚至可以进行暴力模式攻击，破解密码只是一个时间问题。

账户锁定策略可用于域账户和本地用户账户，用来确定某个账户被系统锁定的情况和时间长短。通过包括复位账户锁定计数器、账户锁定时间和账户锁定阈值 3 个策略。而设置账户锁定策略的第一步就是指定账户锁定阈值，即锁定前该账户的无效登录次数。

一般来讲，对于操作失误造成的登录失败次数是有限的。如设置锁定阈值为 3，表示只允许 3 次登录尝试，一旦 3 次登录尝试全部失败，就会锁定该账户。一旦账户被锁定后，即使是合法的用户也无法再次使用该账户。只有管理员才可以重新启用该账户，这就会对用户造成许多不便。为此，可以同时设置锁定的时间和复位计数器的时间。

通过账号锁定策略，可以有效地避免自动猜解工具的攻击，同时也会打击那些手动尝试者的耐心和信心。

1. 账户锁定阈值

该安全策略可以确定造成用户账户被锁定的登录失败尝试的次数。在锁定时间内，无法使用被锁定的账户，除非管理员进行了重新设置或该账户的锁定时间已过期。登录尝试失败的范围可设置为 0～999 之间，建议值为 3～5，这样既允许用户输入或记忆错误，又避免了恶意用户反复尝试使用不同的密码登录系统。

如果要指定账户锁定阈值，只需在【本地安全策略】窗口中的【账户锁定策略】列表中，双击【账户锁定阈值】选项，在弹出对话框的【次无效登录】文本框中输入数字，如 3。然后，单击【确定】按钮，如图 5-9 所示。

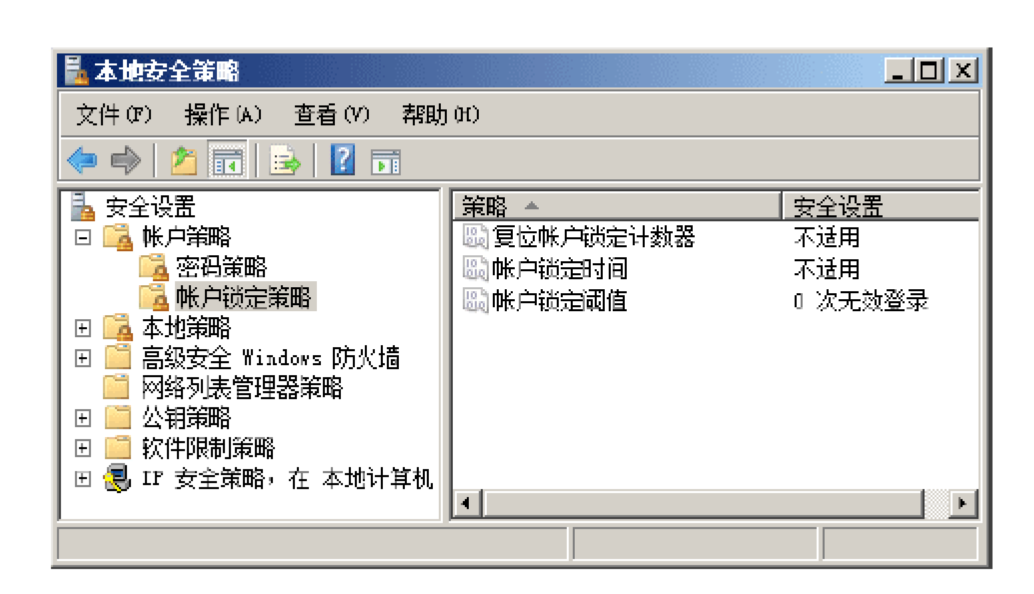
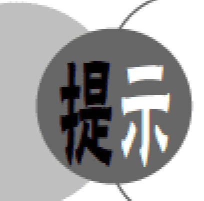


图 5-8　账户锁定策略



图 5-9　设置账户锁定阈值



账户锁定阈值策略在默认状态下被禁用，但从网络安全的角度来讲，为了防止黑客的恶意攻击，通常建议启用该策略，并设置合理的数值。

2. 账户锁定时间

该安全策略可以确定锁定的账户在自动解锁前保持锁定状态的时间（分钟）。锁定时间的有效范围在 0～99999 分钟之间，如果将账户锁定时间设置为 0，那么在管理员明确将其解锁前，该账户将一直被锁定。

如果定义了账户锁定阈值，则账户锁定时间必须大于或等于重置时间。在【本地安全策略】窗口中的【账户锁定策略】列表中，双击【账户锁定时间】选项，在弹出对话框的【账户锁定时间】文本框中，输入账户锁定时间，并单击【确定】按钮，图 5-10 所示为在启用账户锁定阈值后，系统默认账户锁定时间。

3. 复位账户锁定计数器

该安全策略可以确定在登录尝试失败计数器被复位为 0（即 0 次失败登录尝试）之前，尝试登录失败之后所需要的时间（分钟）。该时间的有效范围在 1～99999 分钟之间。

如果定义了账户锁定阈值，那么该复位时间必须小于或等于账户锁定时间。如果要设置复位时间，需要在【本地安全策略】窗口中的【账户锁定策略】列表中，双击【复位账户锁定计数器】选项，在弹出对话框的【在此后复位账户锁定计数器】文本框中，输入复位时间，并单击【确定】按钮，图 5-11 所示为系统默认设置时间，即在 30 分钟之后复位被锁定的账户。



图 5-10　设置账户锁定时间

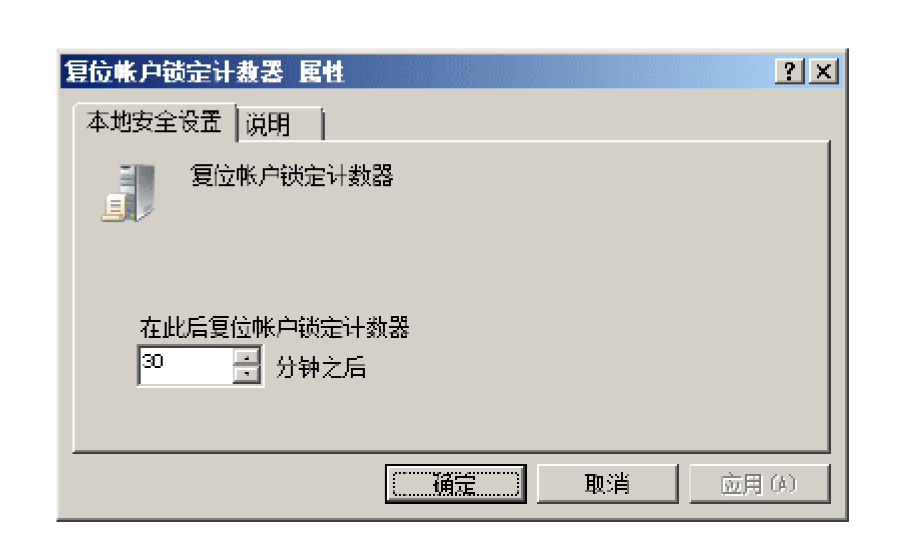
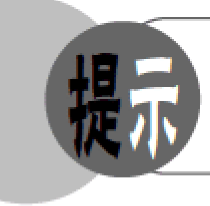


图 5-11　设置锁定账户复位时间

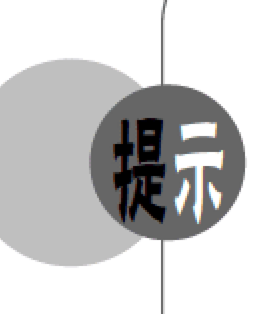


设置复位账户锁定计数器和账户锁定时间的作用相同。

5.1.3　推荐的账户策略设置

通常为了保护用户账户的安全性，推荐的密码策略和账户策略包括以下几方面内容。

- **密码必须符合复杂性要求**　必须启用该策略。
- **密码长度最小值**　设置为 8 个字符或者更高。
- **账户锁定阈值**　设置为 3 次（或者略高）为无效登录。
- **复位账户锁定计数器**　设置为 30 分钟（默认值，可根据实际需要更改）之后。



密码的复杂性是指密码中必须包含字母、数字、特殊符号等内容。在安全性要求比较高的地方，推荐使用超过 12 位以上的密码。密码应该经常更换，特别是除管理员外还有他人知道的情况下。另外，管理员 Administrator 密码建议仅有管理员本人知道并且是足够强壮的密码，且可修改默认的用户名。

5.2 审核策略

审核是 Windows Server 2008 系统安全策略的一部分，它是一个维护系统安全性的工具。通过设置审核策略，确定是否将安全事件记录到计算机上的安全日志中，同时也确定是否记录登录成功或登录失败，或两者都记录。当系统管理员希望了解系统运行状态时，通过查看相关类型的系统事件即可，相对于大量的系统事件信息而言，审核策略产生的日志数量非常少，这大大减少了管理员的工作负担。

5.2.1 审核策略设置

在加入域中的成员服务器和工作站上，默认没有定义事件类别的审核设置。在域控制器中，默认也没有开启审核功能，需要管理员手动启动审核策略。通过为特定的事件类别定义审核设置，可以为单位或公司创建一个适合自身需要的审核策略。

在 Windows Vista 之前，所有安全事件都属于 9 种审核策略之一。通过启用一个审核类别的成功或失败审核，就启用了该类别的所有审核事件。在 Windows Vista 和 Windows Server 2008 中，所有安全事件都归属于一个审核策略子类别。当启用了某个子类别的审核策略后，也就启用了所有属于该子类别的事件。每个子类别的设置中，既有启用由成功的活动生成的事件，也有启用由失败的事件生成的事件。

1. 审核账户登录事件

审核账户登录事件设置确定是否审核在这台计算机用于验证账户时，用户登录到其他计算机或者从其他计算机注销的每个实例。当在域控制器中对域用户账户进行身份验证时，将产生账户登录事件，该事件被记录在域控制器的安全日志中。当在本地计算机上对本地用户进行身份验证时，将产生登录事件，该事件被记录在本地安全日志中，不产生账户注销事件。

如果需要定义该策略，可以指定是否审核成功、审核失败或根本不对事件类型进行审核。当某个账户登录成功时，成功审核策略会产生审核项；当某个账户登录失败时，失败审核会生成审核项。

首先，执行【开始】|【管理工具】|【本地安全策略】命令，在打开的窗口中，展开【本地策略】节点，选择【审核策略】选项。然后，在右侧窗格中，双击【审核账户登录事件】选项，如图 5-12 所示。

通常外来入侵不会一次就能登录成功，因此，一般只需要记录失败事件即可。在弹出的【审核账户登录事件 属性】对话框中，可以禁用【成功】复选框，并单击【确定】按钮，如图 5-13 所示。当然，为了更加安全，也可以保持默认设置。如果同时禁用【成功】和【失败】复选框，则表示无审核。

2. 审核账户管理

审核账户管理设置确定是否审核计算机上的每一个账户管理事件。账户管理事件包括以

下几种。

图 5-12 【本地安全策略】窗口

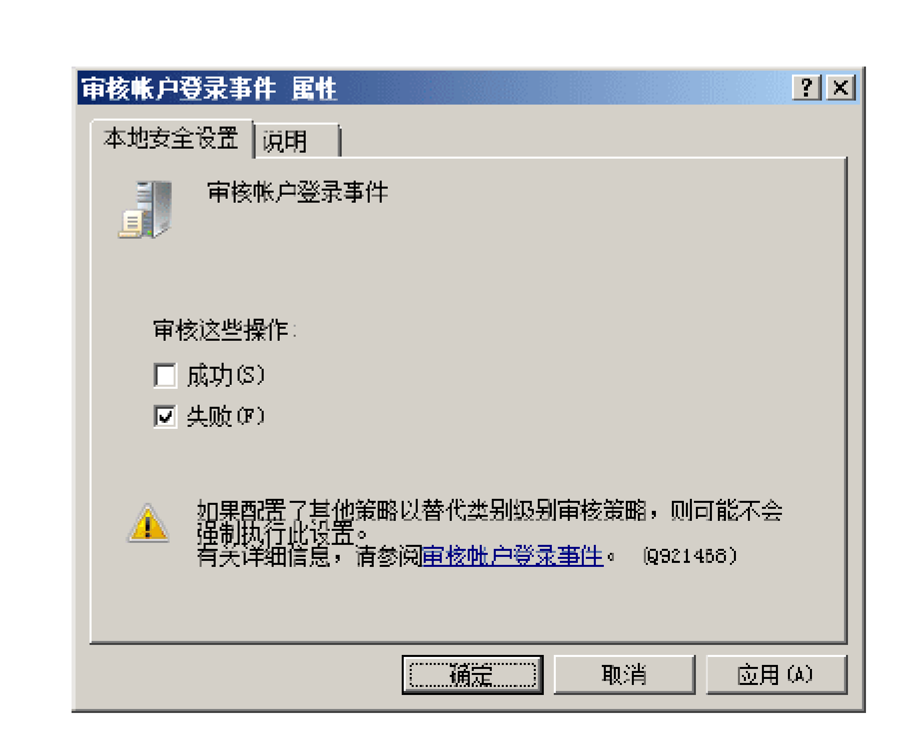


图 5-13　审核账户登录事件策略

- ❑ 创建、更改或删除用户账户或组。
- ❑ 重命名、禁用或启用用户账户。
- ❑ 设置或更改密码。

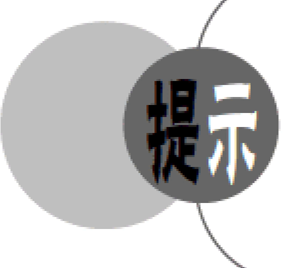
如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。任何账户管理事件成功时，成功审核都会产生审核项；任何账户管理事件失败时，失败审核也都会生成审核项。

3. 审核目录服务访问

审核目录服务访问设置审核用户访问那些指定资金的系统访问控制列表(SACL)的 Active Directory 对象的事件。

默认情况下，在“默认域控制器组策略对象（GPO）”中该值设置为无审核，并且在该值没有任何意义的工作站和服务器中，它都保持未定义状态。

如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。用户成功访问指定了 SACL 的 Active Directory 对象时，成功审核会生产审核项。用户尝试访问指定了 SACL 的 Active Directory 对象失败时，失败审核会生成审核项。



通过使用某个 Active Directory 对象属性对话框中的【安全】选项卡，可以设置该对象的 SACL。该操作与审核对象访问相同，只不过仅应用于 Active Directory 对象而不是文件系统和注册表对象。

4. 审核登录事件

审核登录事件审核每一个登录或注销计算机的用户实例。

在域控制器中将生成域账户活动的账户登录事件，并在本地计算机中生成本地账户活动的账户登录事件。如果同时启用账户登录和账户审核策略类别，那么使用域账户的登录将生成登录或注销工作站或服务器的事件，而且将在域控制器中生成一个账户登录事件。另外，在用户登录而检索登录脚本和策略时，使用域账户的成员服务器或工作站的交互式登录将在

域控制器上生成登录事件。

如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。登录成功时，成功审核会生成审核项。登录失败时，失败审核会生成审核项。

5. 审核对象访问

审核对象访问审核用户访问某个对象的事件，如文件、文件夹、注册表项和打印机等，它们都拥有自己特定的系统访问控制列表（SACL）。

如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。当用户成功访问指定了 SACL 的对象时，成功审核将生成审核项。当用户尝试访问指定了 SACL 的对象失败时，失败审核也会生成审核项。

6. 审核策略更改

审核策略更改审核用户权限分配策略、审核策略或信任策略更改的每一个事件。

如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。对用户权限分配策略、审核策略或信任策略所作更改成功时，成功审核会生成审核项。对用户权限分配策略、审核策略或信任策略所作更改失败时，失败审核会生成审核项。

7. 审核特权使用

审核特权使用审核用户实施其权力的每一个实例。

如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。用户权力实施成功时，成功审核会生成审核项。用户权力实施失败时，失败审核会生成审核项。

8. 审核进程跟踪

审核进程跟踪审核事件（如程序激活、进程退出、句柄复制和间接对象访问等）的详细跟踪信息。

如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。所跟踪的过程成功时，成功审核会生成审核项。所跟踪的过程失败时，失败审核会生成审核项。

9. 审核系统事件

当用户重启或关闭计算机时或者是对系统安全或安全日志有影响的事件发生时，安全设置确定是否予以审核。

如果定义该策略，可以指定是否审核成功、审核失败或根本不对该事件类型进行审核。系统事件执行成功时，成功审核会生成审核项。系统事件执行失败时，失败审核会生成审核项。

5.2.2 推荐的审核策略设置

Windows Server 2008 提供 9 种类型的事件审核策略，对于每一类都可以指明是审核成功

事件、失败事件，还是两者都审核，但对于安全性较高的网络来讲，通常有如下推荐的审核策略设置。

❑ **审核策略更改**

确定是否对用户权限分配策略、审核策略或信任策略更改的每一个事件进行审核。系统默认设置为“成功”，建议设置为“成功”和“失败”。只需在【审核策略更改 属性】对话框中，同时启用【失败】复选框即可，如图 5-14 所示。

❑ **审核登录事件**

确定是否审核用户登录到计算机，从该计算机注销或建立与该计算机网络连接的每一个实例。如果设置为审核“成功”，可用来确定哪个用户成功登录到哪一台计算机；如果设置为审核“失败”，虽然可以用来检测入侵，但攻击者生成的大量登录失败日志，会造成拒绝服务（DoS）状态。建议保持系统默认设置即可，如图 5-15 所示。



图 5-14　审核策略更改设置

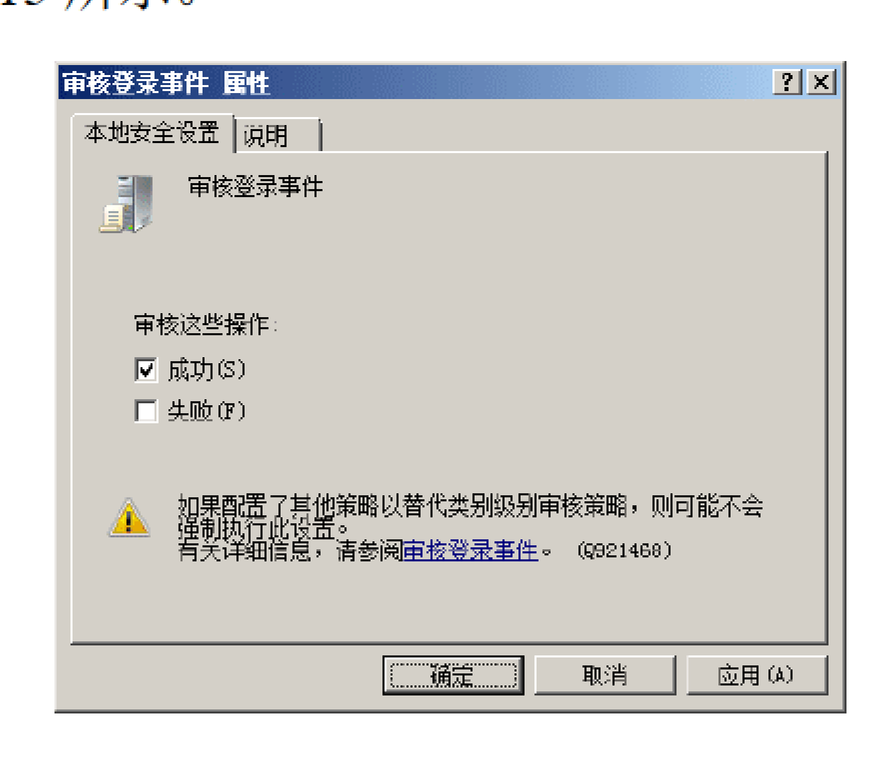


图 5-15　审核登录事件策略

❑ **审核对象访问**

由于这些对象，如文件、文件夹、注册表项等，都指定了自己的系统访问控制列表（SACL）的事件，因此建议设置为“成功”。即在【审核对象访问 属性】对话框中，禁用【成功】复选框，而启用【失败】复选框，如图 5-16 所示。

❑ **审核进程跟踪**

确定是否审核事件的详细跟踪信息，如程序激活，进程结束等。当怀疑系统被攻击时，通常启用该策略，系统默认设置为“成功”。

❑ **审核目录访问服务**

由于在启用该策略后，会在域控制器的安全日志中生成大量审核项，因此只有在确实要使用所创建的信息时才启用。系统默认设置为“成功”，但在不需要使用时，建议禁用【成功】和【失败】复选框，如图 5-17 所示。

❑ **审核特权使用**

该策略用于确定是否对用户行使用户权限的每个实例进行审核，建议设置为“失败”，如图 5-18 所示。

❑ **审核系统事件**

用于确定当用户重启或关闭计算机时，或者对系统安全或安全日志有影响的事件发生时，是否予以审核。由于这些事件是非常重要的，因此建议设置为“成功”和“失败”。

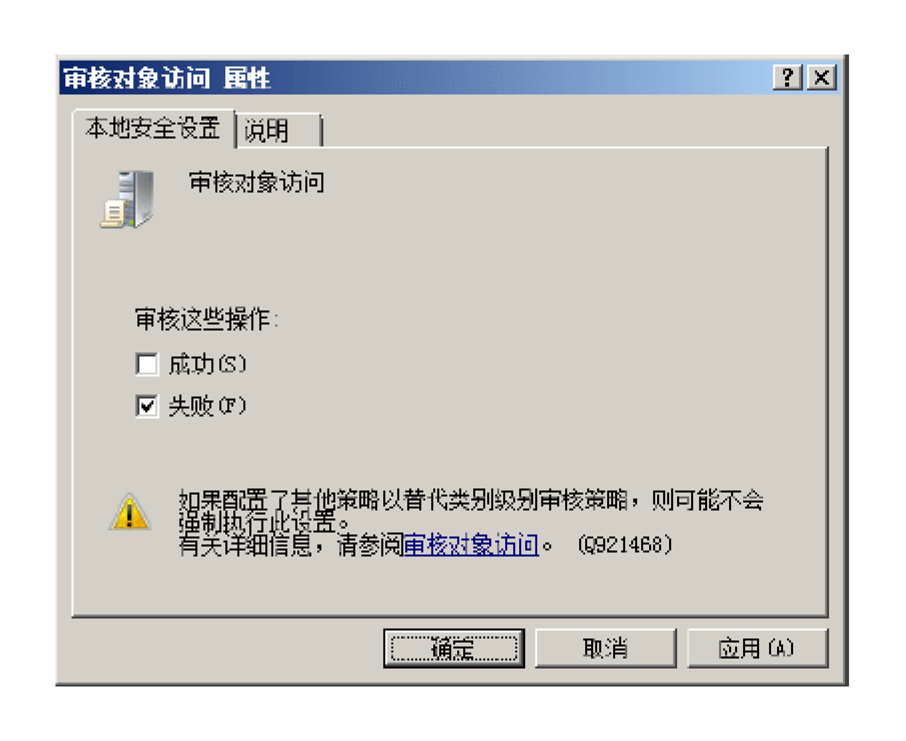


图 5-16　审核对象访问策略

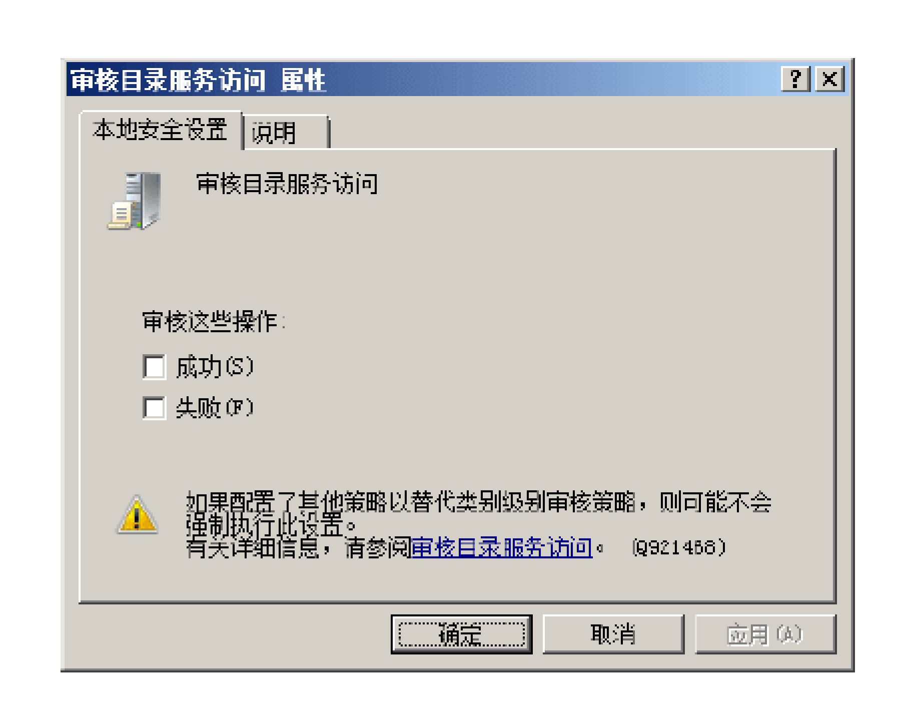


图 5-17　审核目录访问服务策略

❑ 审核账户登录事件

该策略可以确定当用户登录到其他计算机或从中注销时，是否进行审核，该信息对于管理员十分重要，因此建议设置为“成功”和“失败”。系统默认仅启用【成功】复选框，同时启用【失败】复选框即可，如图 5-19 所示。

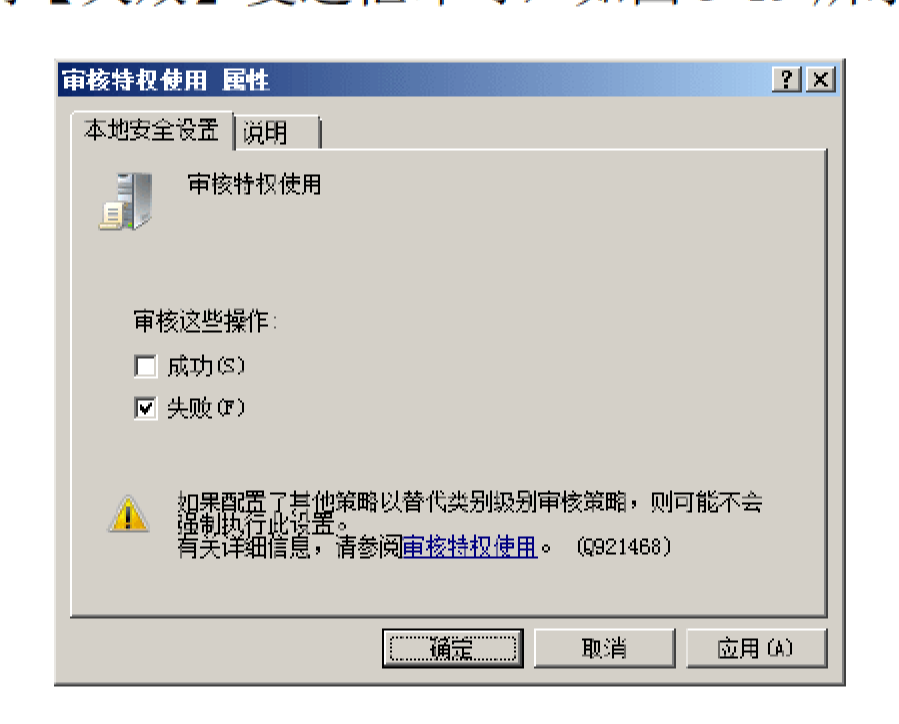


图 5-18　审核特权使用策略

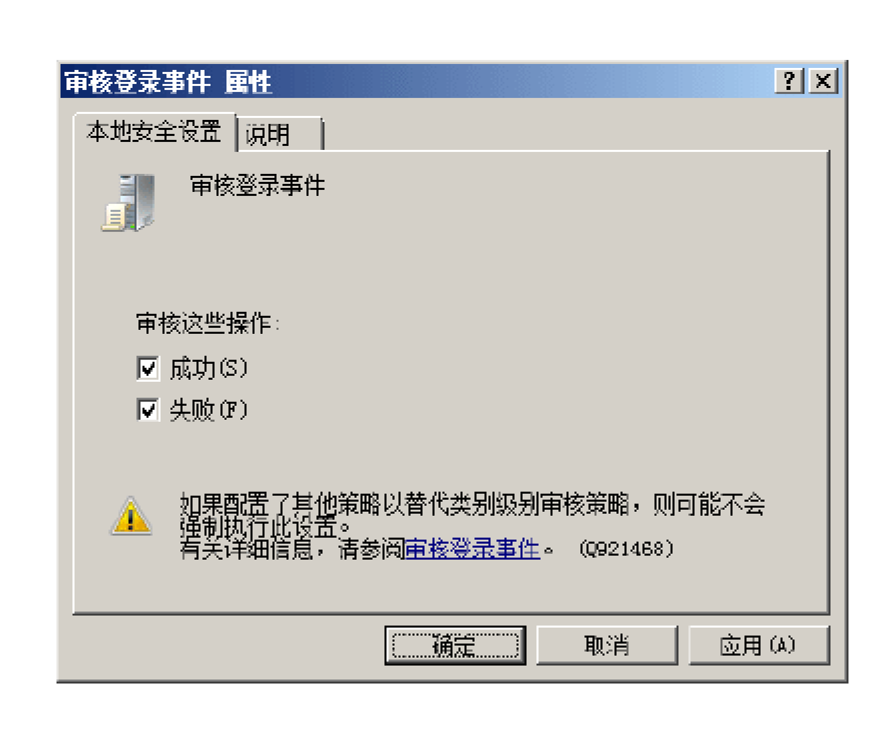


图 5-19　审核账户登录事件

❑ 审核账户管理

用于确定是否对计算机上的每个账户管理事件（如重命名、禁用等）进行审核，建议设置为“成功”和“失败”，如图 5-20 所示。

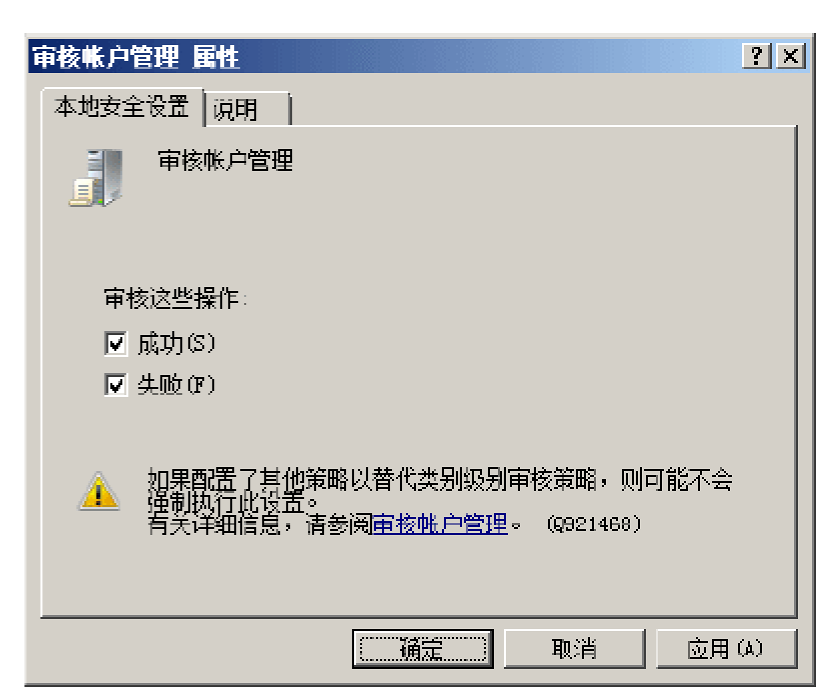


图 5-20　审核账户管理

5.2.3　调整日志审核文件的大小

在安装 Windows Server 2008 时，系统默认设置了日志文件的大小，例如，应用程序日志、安全日志、系统日志等日志的默认大小均为 20480KB。管理员可以手动设置日志文件的大小。

Windows 日志类别包括早期版本的 Windows 中可用的日志（应用程序、安全和系统日志）。另外，还包括两个新的日志类别，即安装程序日志和转发的事件（Forwarded Events）日志。Windows 日志用于存储来自旧版应用程序的事件以及适用于整个系统的事件。

在 Windows Server 2008 中，系统日志通常包括如下 4 种类型。

❑ **应用程序日志**

应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误。应用程序开发人员决定记录哪些事件。

❑ **安全日志**

安全日志包含诸如有效和无效的登录尝试等事件，以及记录与资源使用相关的事件，如创建、打开或删除文件或其他对象。管理员可以指定在安全日志中记录什么事件。例如，如果已启用登录审核，则对系统的登录尝试将记录在安全日志中。

❑ **系统日志**

系统日志包含 Windows 系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。服务器预先确定由系统组件所记录的事件类型。

❑ **安装程序日志**

安装程序日志包含与应用程序安装关的事件。例如，安装系统或者安装微软公司的产品。

另外，当一台计算机安装 Windows Server 2008 操作系统，且被配置为域控制器时，通常使用以下 3 种日志来记录事件。

❑ **目录服务日志**

目录服务日志包含 Active Directory 服务记录的事件。例如，在目录服务日志中记录服务器和全局编录间的连接问题。

❑ **文件复制服务日志**

该日志包含 Windows 文件复制服务记录的事件。例如，在文件复制日志中，记录文件复制失败和域控制器（利用关于系统卷更改的信息）更新时发生的事件。运行 Windows 并配置为域名系统（DNS）服务器的计算机在其他日志中记录事件。

❑ **DNS 服务器日志**

DNS 服务器日志包含 DNS 服务记录的日志。

除此之外，还包括应用程序和服务日志，它是一种新类别的事件日志。这些日志存储来自单个应用程序或组件的事件，而不是那些可能影响整个系统的事件。应用程序和服务日志包括以下 4 种不同类型的事件。

❑ **管理事件**

该类事件主要以最终用户、管理员和技术支持人员为目标。例如，应用程序无法连接到打印机时所发生的事件。这些事件或者有详细的文档记录，或者有与其相关联的消息，通过这些信息可以指导用户进行操作以纠正问题。

❑ **操作事件**

用于分析和诊断问题或发生的事件。这些事件可以被用于分析问题或发生的事件。例如，从系统中添加或删除打印机时所发生的事件

❑ **分析事件**

该事件是大量发生的事件。这些事件描述应用程序操作并指示用户干预其无法处理的问题。

❑ **调试事件**

该事件主要由开发人员用于解决其程序中存在的问题。

系统日志有很重要的作用，如何妥善保存这些日志记录，是管理员日常维护的一项重要工作。在默认状态下，系统日志的存储空间、保存方法及保存日期都是有一定限制的，如果系统事件较多，时间久了很可能会造成存储溢出，即导致部分事件记录被自动清除。因此，调整日志审核文件的大小很有必要。

通常，在业务应用系统中建议增大日志文件的大小，日志文件的最大值为 512000KB（512MB）。然而，在实际环境中，不建议使用如此大的日志文件，在进行日志筛选和导出的时候，需要占用大量的时间，同时在日志写入的时候，系统还需要对文件进行更新，因此，会消耗大量的服务器资源。下面就以调整“安全”日志为例进行说明。

首先，执行【开始】|【管理工具】|【事件查看器】命令，在打开的【事件查看器】窗口中，展开【Windows 日志】节点，右击【安全】选项，并执行【属性】命令，如图 5-21 所示。

在弹出的【日志属性-安全（类型：管理的）】对话框中的【日志最大大小（KB）】文本框中，输入要设置的日志文件的大小值，并单击【确定】按钮，如图 5-22 所示。系统默认设置日志最大大小为 20480KB。



图 5-21　【事件查看器】窗口

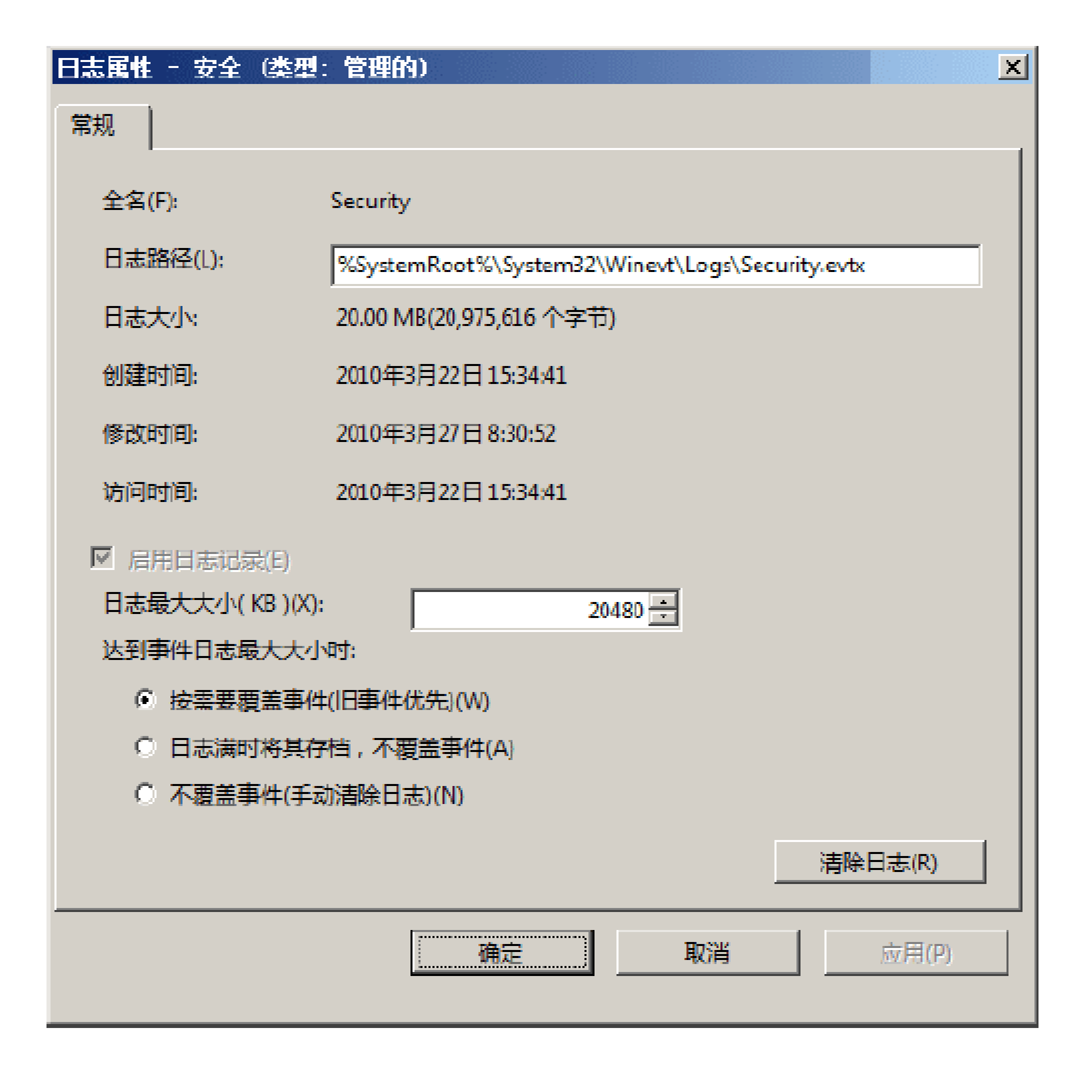
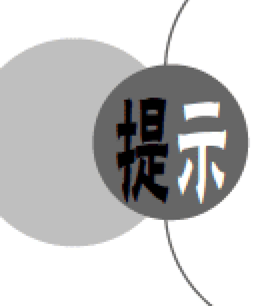


图 5-22　设置日志最大大小

对于该对话框中的各选项有如下说明。

- **日志路径**　当前日志的保持路径。
- **日志最大大小**　当前事件日志在计算机磁盘中被划分的磁盘空间，可以根据服务器类型判断日志文件的大小，从而设定合适的空间上限。
- **达到事件日志最大大小**　当达到日志大小上限时系统将按照默认或预先设定的动作执行，系统默认已选中【按需要覆盖事件（旧事件优先）】单选按钮。



所设置日志文件的大小必须为 64KB 的整数倍，且不能小于 1024KB。如果是手动键入日志大小而没使用微调控件，则会将其取整为最接近的 64KB 的倍数值。另外，如果所设置的日志大小最大值小于当前的日志大小，那么设置的最大值将直到清除日志时才生效。

5.3　限制用户登录

在单位或公司内部网络中，为了进一步保证用户的账户安全，可以通过对用户的登录行为进行限制来实现。这样，即使是密码被泄露，系统也可以在一定程度上阻止黑客的入侵。对于 Windows Server 2008 网络来讲，可以使用 Active Directory 用户和计算机管理单元来限制用户的登录行为，也可以使用组策略提供的登录权利功能，来限制用户的登录和访问。

5.3.1　用户权限

管理员可以指派特定权利组账户或单个用户账户。用户执行特定任务的权利，如交互式登录系统或备份文件和目录等，通常会影响整个计算机系统，而不只是某个目录对象。用户权利与权限不同，用户权利适用于用户账户，而权限则附加给对象。

1. 用户权利

用户权利是一种定义在本地级别上的功能。虽然它可以应用于单个的用户账户，但最好是在组账户的基础上对其进行管理。这样可以确保作为组成员登录的账户将自动继承该组的相关权利。通过对组而不是对单个用户指派用户权利，可以简化用户账户管理的任务。当组中的用户都需要相同的用户权利时，可以一次对该组指派用户权利，而不是重复地对每个单独的用户账户指派相同的用户权利。

对组指派的用户权利应用到该组的所有成员。如果一个用户属于多个组，则用户权利是叠积的，也就是说用户有多个组的用户权利。指派给某个组的用户权利只有在特定的情况下才会与指派给其他组的用户权利发生冲突。然而，指派给某个组的用户权利通常不会与指派给其他组的用户权利发生冲突。要删除用户的权利，只需将其从所属的组中删除即可。在此情况下，用户不再拥有指派给这个组的权利。

通常包括如下两种类型的用户权利。

- **特权**　如备份文件和目录的权利。
- **登录权利**　如登录到本地系统的权利。

权限可以授权对不同对象的不同访问，而权利却能够给予一个用户做特殊任务的权利。通常情况下，权利倾向于特定的系统上，例如用户登录到该系统的权利，修改系统时间的权利以及关闭系统的权利等。

另外，有些权利基本上是系统专用的能力，可以不考虑访问控制列表。例如备份文件，显然，如果不能读取这些文件就不能对这些文件进行备份，但是具有备份权利的用户能备份系统上的任何文件，包括那些拒绝访问的文件。权利大于权限，但不需要担心文件的安全性，因为备份组的权利只有在备份时才有效，如作为备份组的成员不能打开服务器上的文件并读取其中的内容。

2. 特权

特权控制对计算机系统范围的资源的访问，并可以覆盖在特定对象上设置的权限。例如，

用户作为备份组的成员登录到域时，具有对所有域服务器执行备份操作的权利。但是，这要求能够读取这些服务器上的所有文件，甚至是文件所有者已经明确设置对所有用户（包括备份组成员）都拒绝访问的文件。在这种情况下，执行备份的用户权利优先于所有的文件和目录权限。

3. 登录权利

登录权利是指分配给用户，并指定用户以哪种方式登录系统的用户账户权利。表 5-2 所示为默认的登录权利。

表 5-2　默认登录权利

登录权利	说明	默认设置
从网络访问计算机	允许用户通过网络连接到计算机	管理员、每个人、用户、高级用户和备份操作员
允许通过终端服务登录	允许用户通过远程桌面连接登录到本计算机	管理员和远程桌面用户
作为批处理作业登录	允许用户使用批处理查询工具登录，如果安装了 Internet 信息服务（IIS），则系统将权利自动分配给匿名访问 IIS 的内置账户	没有任何用户账户
作为服务登录	允许某种安全原则以服务身份登录。可以将服务配置为在 Local System、Local Service 或 Network Service 账户下运行，这些账户具有作为服务登录的内置权利。在单个账户下运行的任意服务都必须授予该权利	没有任何用户账户
本地登录	允许用户通过计算机键盘操作	管理员、高级用户、用户、来宾和备份操作员
拒绝从网络访问这台计算机	禁止用户或组从网络连接到本计算机	没有任何用户账户
拒绝本地登录	禁止用户或组直接通过键盘登录	没有任何用户账户
拒绝作为批处理作业登录	禁止用户或组通过批处理队列工具登录	没有任何用户账户
拒绝作为服务登录	禁止用户或组作为服务登录	没有任何用户账户
拒绝通过终端服务登录	禁止用户或组作为终端服务客户登录	没有任何用户账户

特殊用户账户 LocalSystem 具有已指派给它的几乎所有特权和登录权利，因为作为操作系统的一部分运行的所有进程都与该账户相关，而这些进程都需要全部的用户权利。

4. 将用户权利指派到组

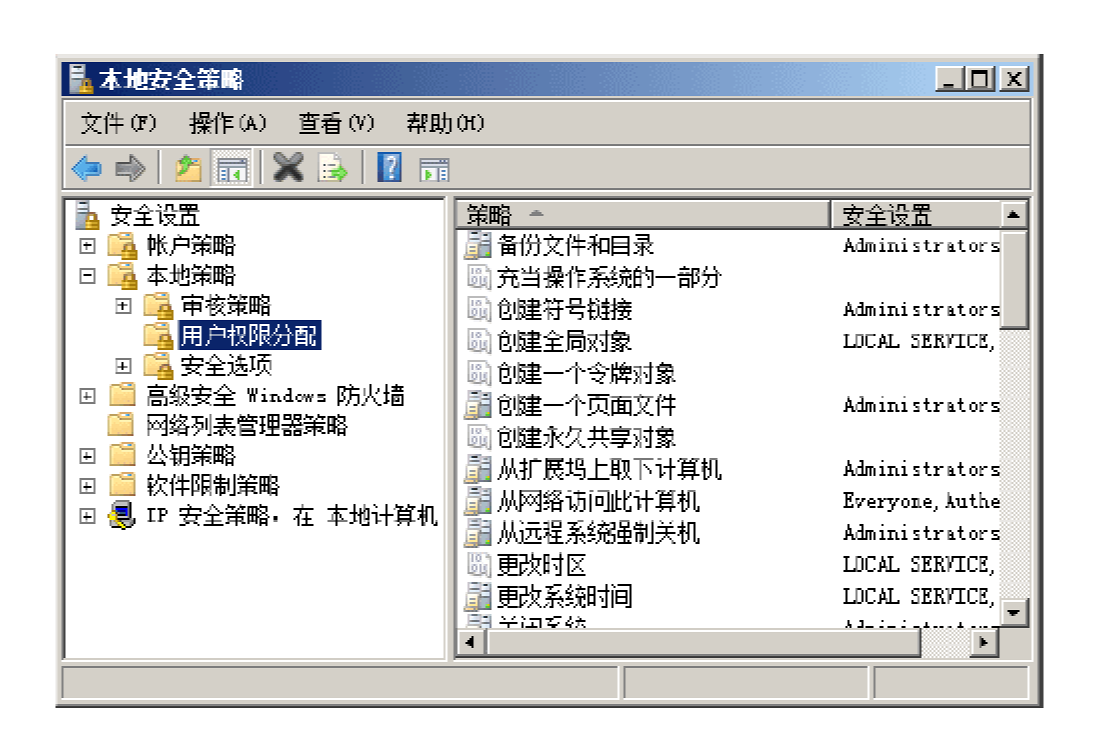
为减轻用户账户的管理任务，避免权限管理混乱，应该将用户的权利指派到组，然后将需要获得此权限的用户添加到该组中，尤其是对于用户较多的大型网络，更应该如此。

在 Windows Server 2008 域网络中，可以通过在域控制器的组策略管理控制单元、编辑域控制器的默认策略（Default Domain Controllers Policy）或者本地安全策略中进行设置。如果

是独立服务，则只能通过本地安全策略管理单元进行设置。

在 Windows Server 2008 域控制器中，执行【开始】|【管理工具】|【本地安全策略】命令，在打开的窗口中，展开【本地策略】节点，并选择【用户权限分配】选项。然后，在右侧窗格中，可以查看到所有可供分配的用户权限，如图 5-23 所示。

双击需要分配给组的权限（如“从网络访问此计算机”），在弹出的【从网络访问此计算机 属性】对话框中的列表中，可以查看到具有此权利的用户或者组，如图 5-24 所示。





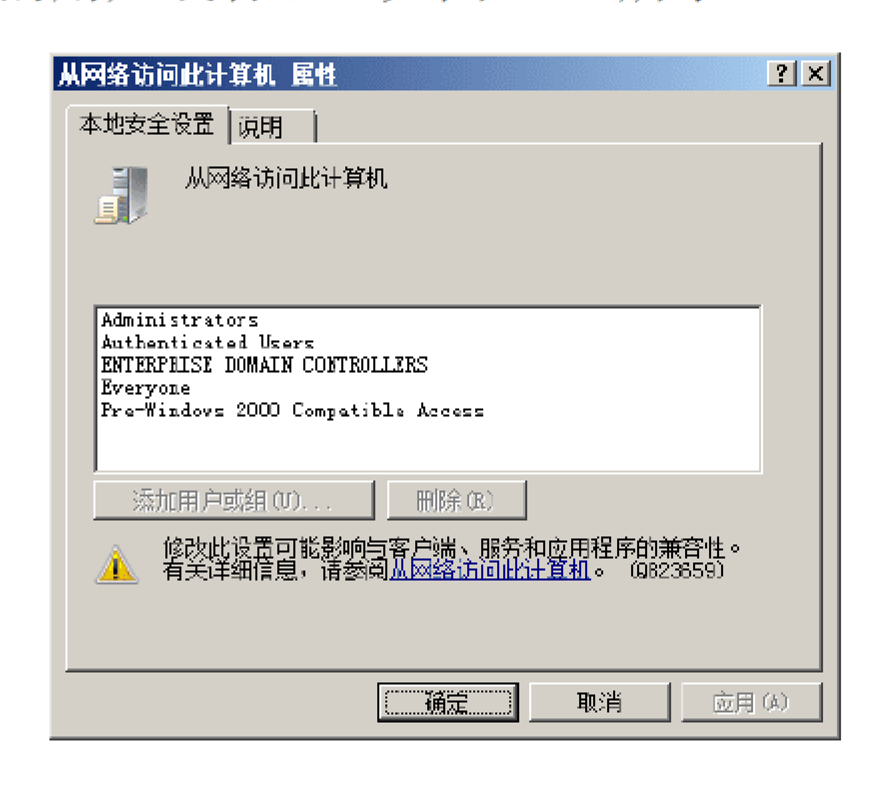


图 5-23 【本地安全策略】窗口　　　　图 5-24 【从网络访问此计算机 属性】对话框

当为组分配某个权限以后，该组中的用户同时也会具有该权限，而以后向该组添加新用户时，新用户也会拥有该权限。

通常，将权限分配给用户组时应注意如下内容。

- ❑ 管理员组（Administrators）可以被授权的权利包括更改系统事件、创建页面文件、安装和卸载设备驱动程序、在本地登录、管理审核安全日志、配置单一进程、配置系统性能、关闭系统、取得文件或者对象的所有权。
- ❑ 备份操作员（Backup Operators）可以被授权的权利包括备份文件和目录、在本地登录、还原文件和目录。
- ❑ 用户组可以被授权的权利为在本地登录（默认）。
- ❑ 将有关 Everyone 组的权利删除。尤其是在 Windows 2000 系统中，默认情况下，该组被赋予“完全控制”权限，这对于系统安全是不利的。

5.3.2　限制登录

登录权限控制为谁授予登录计算机的权限以及他们的登录方式。在网络中，为了增加系统的安全性，通常会限制某些用户的登录以保护网络内部敏感数据的安全性。

对用户进行限制登录可以通过该用户账户的属性对话框来完成，通常包括登录时间、登录到、账户等多个方面的限制。

在 Windows Server 2008 域控制器中，如果要设置限制登录，首先需要执行【开始】|【管理工具】|【Active Directory 用户和计算机】命令，在打开的窗口中，展开 slkj.com 节点，并选择 Users 选项。然后，在右侧窗格中，右击新建的用户账户 ly，并执行【属性】命令，如图 5-25 所示。

在弹出的对话框中，切换到【账户】选项卡，选中【账户过期】栏内的【在这之后】单选按钮，并设置过期时间，如图 5-26 所示。然后，单击【确定】按钮。这样，该用户账户在设定的过期时间之后将不能够再使用。同样，通过该对话框还可以设置用户的登录时间（在哪个时间段允许登录）、登录到哪一台计算机等限制策略。

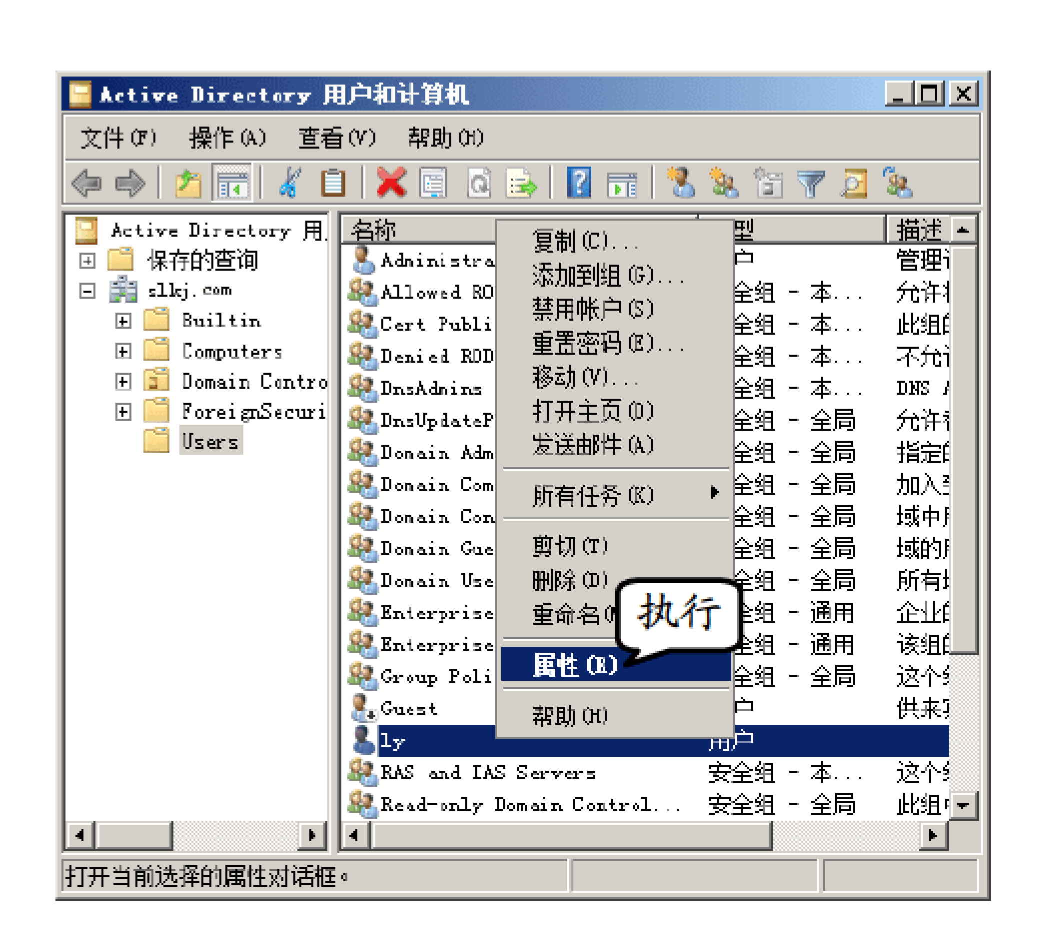


图 5-25 【Active Directory 用户和计算机】窗口

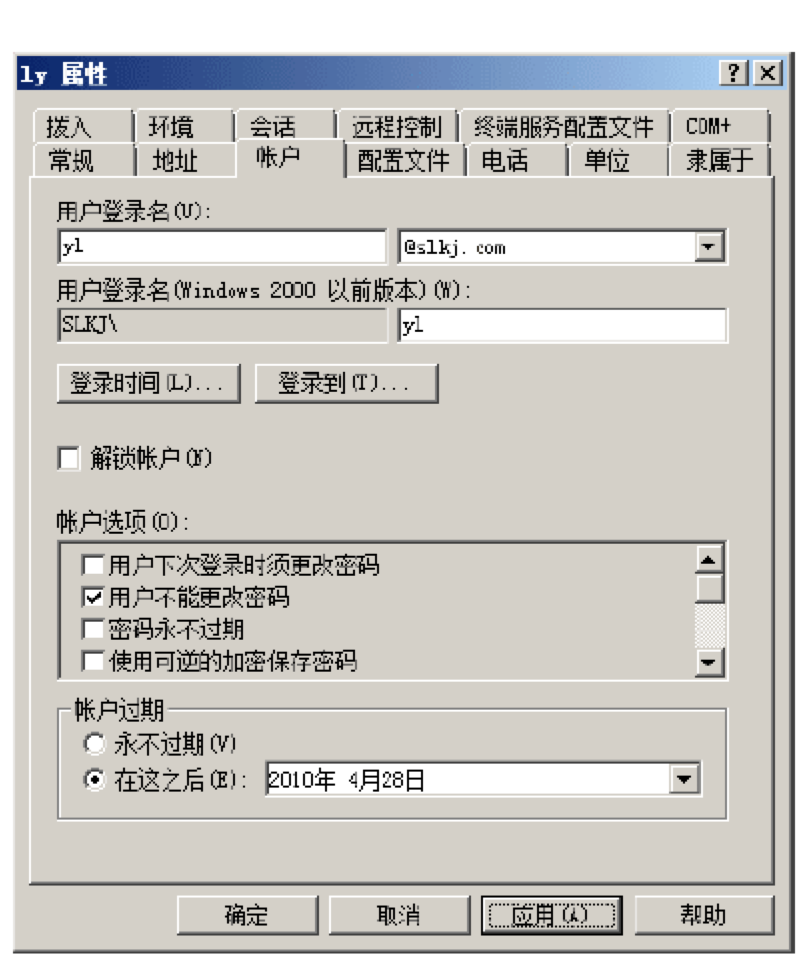


图 5-26 设置账户过期时间

5.4 安全配置和分析

无论对于服务器还是对于客户端，安全都是头等大事。计算机的安全是借助安全配置来实现的。而“安全配置和分析”工具是微软公司提供的简单、快捷的安全配置方法，网络管理员在分析完服务器或者个人计算机的操作系统后，可以根据当前的配置状态，调整当前的配置，然后发布到应用环境中。

5.4.1 预定义的安全模板

在 Windows Server 2008 中，提供了许多增量安全模板。默认情况下，这些模板存放在 Systemroot\Security\Templates 目录中，可以使用“安全模板”管理单元自定义这些模板并将其导入到“组策略”管理单元的“安全设置”扩展中。

通常包括如下几种预定义的安全模板。

- ❑ 默认工作站——basicwk.inf。
- ❑ 默认服务器——basicsv.inf。
- ❑ 默认域控制器——basicdc.inf。
- ❑ 兼容工作站或服务器——compatws.inf。
- ❑ 安全工作站或服务器——securews.inf。
- ❑ 高度安全工作站或服务器——hisecws.inf。

- 专用域控制器——dedicadc.inf。
- 安全域控制器——securedc.inf。
- 高度安全域控制器——hisecdc.inf。

5.4.2　安全等级

常规分析作为企业风险管理程序的一部分，允许网络管理员跟踪并确保在每台计算机上有足够的安全级别。而在预定义的安全模板中包括基本、兼容、安全、高度安全和专用域控制器 5 个公用安全等级。

1. 基本（Basic*.inf）等级

基本配置的模板可以作为一种方法提供以反转不同安全配置的应用程序。除了这些属于用户的权限之外，基本配置可以将 Windows Server 2008 默认的安全设置应用于所有安全区域。因为应用程序安装程序通常会修改用户权限以成功地使用应用程序，所以不在基本模板中进行修改。撤销这些修改并不是基本配置文件的目的。

2. 兼容（Compat*.inf）等级

Windows Server 2008 默认的安全配置为本地 Users 的成员设置了严格的安全性，而本地 Power Users 的安全设置与 Windows NT 4.0 兼容。这一默认配置允许在提供给 Users 的标准 Windows 环境中运行经 Windows Server 2008 验证过的应用程序，同时还允许在提供给 Power Users 的安全性稍低的环境下运行未经 Windows Server 2008 验证的应用程序。但是，如果为了运行未经 Windows Server 2008 验证过的程序而让用户成为 Power Users 组的成员，这对某些环境就太不安全了。因此，在默认情况下，只将用户指派为 Users 的成员，然后将 Users 的安全性特权级降至 Windows Server 2008 未验证的应用程序也可以运行，Windows Server 2008 为这样的组织设计了兼容模板。通过降低通常由应用程序访问的特定文件、文件夹和注册表项的安全级别，兼容模板允许大多数的应用程序成功运行。此外，由于假定应用兼容模板的网络管理员不需要用户成为 Power Users，因此将删除 Users 的所有成员。

3. 安全（Secure*.inf）等级

除文件、文件夹和注册表项外，安全模板是对所有的安全区域执行推荐的安全设置。因为默认情况下将安全地配置文件系统和注册表权限，所以这些都不会被修改。

4. 高度安全（Hisec*.inf）等级

高度安全模板定义 Windows Server 2008 网络通信的安全设置。设置安全区域以便为用于运行 Windows Server 2008 的计算机间的网络通信和协议求最大限度的保护。它们不能同时运行 Windows 95/98/Me 或 Windows NT 的计算机进行通信。

5. 专用域控制器（Dedica*.inf）等级

在默认情况下，运行 Windows Server 2008/2003 域控制器上的本地用户安全并不理想。这

允许网络管理员以向后兼容的方式运行域控制器上现有的基于服务器的应用程序（不推荐）。如果不运行域控制器上基于服务器的应用程序（推荐），默认的本地用户组文件系统和注册表权限可以按照与 Windows Server 2008/2003 工作站和独立服务器默认定义相同的方式定义。通过执行专用安全模板，这些理想的本地用户安全设置可以在 Windows Server 2008 域控制器上应用。

5.4.3　实施安全配置和分析

“安全配置和分析”是微软公司提供的一款免费的安全配置工具，如果网络管理员对安全模型和安全理念不熟悉，那么可以使用“安全配置和分析”工具来配置服务器系统安全。

1. 添加安全配置和分析管理单元

在 Windows mmc 管理员控制台中，“安全配置和分析”管理单元默认没有添加，需要网络管理员手动将其添加到控制台中。

首先执行【开始】|【运行】命令，在弹出的对话框中，输入 mmc 命令，在打开的窗口中，单击【文件】菜单，并执行【添加/删除管理单元】命令，如图 5-27 所示。

接着，在弹出对话框中的【可用的管理单元】列表中，选择【安全配置和分析】选项，并单击【添加】按钮。然后，单击【确定】按钮，如图 5-28 所示。



图 5-27　控制台窗口

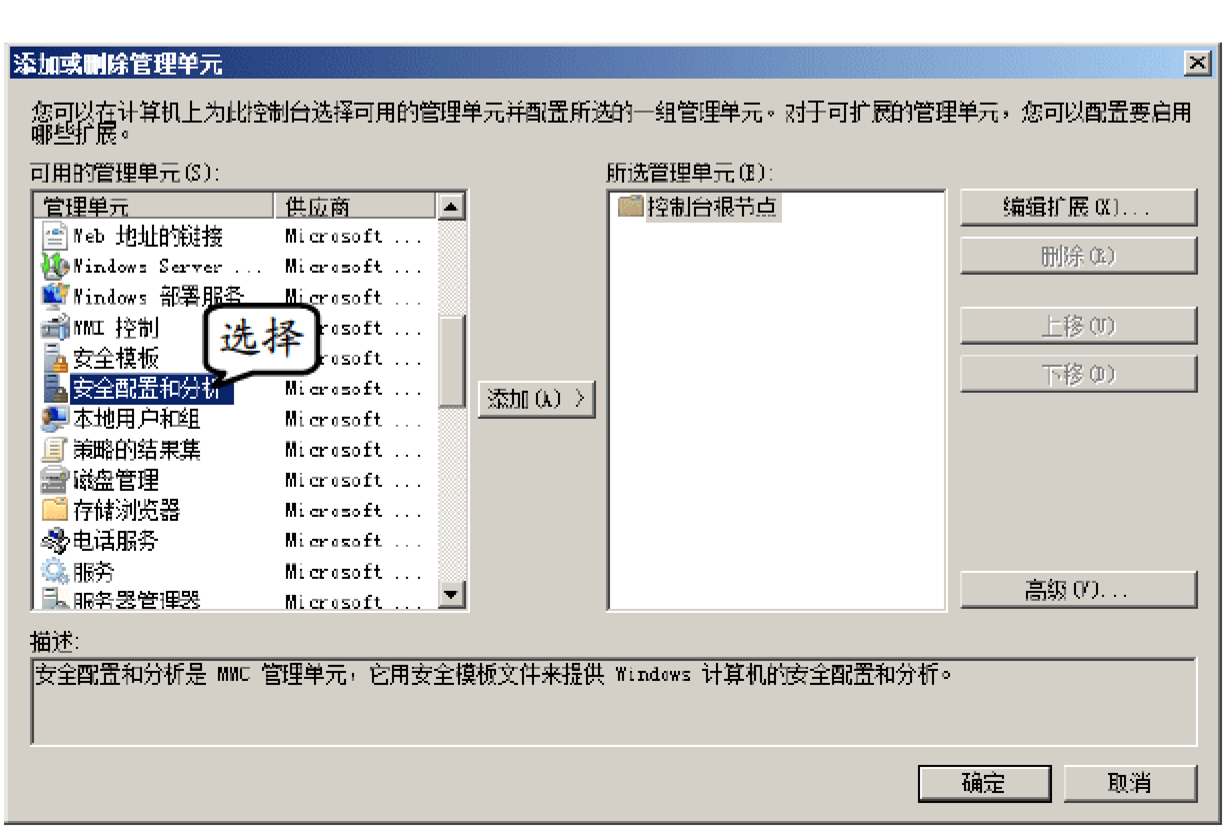


图 5-28　添加安全配置和分析管理单元

2. 设置安全数据库

在默认情况下，【安全配置和分析】控制台中，没有加载任何安全数据库，需要管理员手动设置安全数据库。

在【安全配置和分析】控制台中，右击【安全配置和分析】选项，并执行【打开数据库】命令，如图 5-29 所示。

在弹出的对话框中，选择现有的个人数据库，并单击【打开】按钮，如果没有也可以输入文件名创建新的安全数据库，如图 5-30 所示。

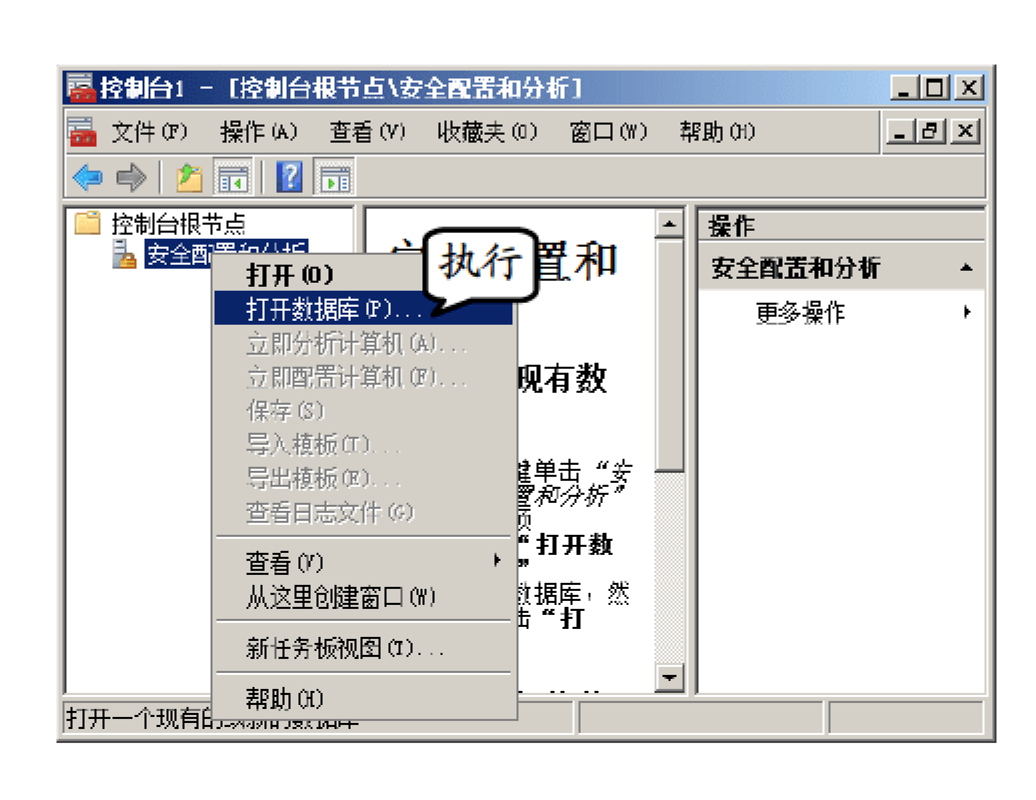


图 5-29　打开数据库

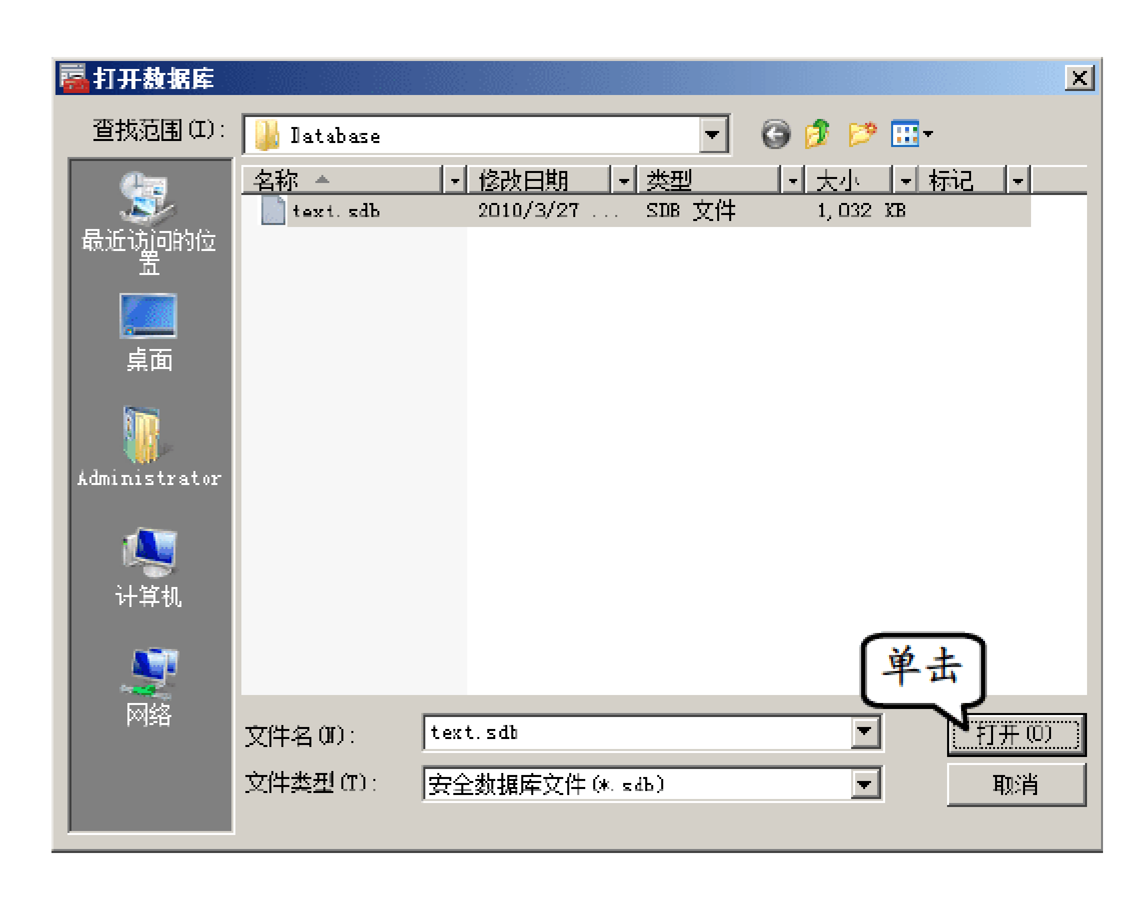


图 5-30　选择数据库

3．分析系统安全性

通过比较系统当前的状态和已导入到数据库中的安全模板，安全配置和分析工具执行安全分析。此模板是基本配置，并且它是包含推荐的系统安全设置的模板。安全配置和分析工具会询问基本配置中所有安全区域的系统安全设置，将找到的值与基本配置进行比较。如果当前的系统设置与基本配置的设置匹配，则假定它们正确。如果不匹配，则将有问题的属性作为需要检查的潜在问题显示。

可以创建数据库，导入模板进行分析，并且可以重复导入并加载多个模板。数据库将各种模板合并以创建一个复合模板，按导入顺序解决冲突；当有冲突时，优先导入最新的模板。一旦将模板导入到选择的数据库，就可以分析或配置系统。

如果要分析系统安全性，首先需要在【安全配置和分析】控制台中，右击【安全配置和分析】选项，并执行【立即分析计算机】命令，如图 5-31 所示。

在【进行分析】对话框中的【错误日志文件路径】文本框中，可以使用默认的错误文件路径，或者输入新的日志的文件名和有效路径，并单击【确定】按钮，如图 5-32 所示。

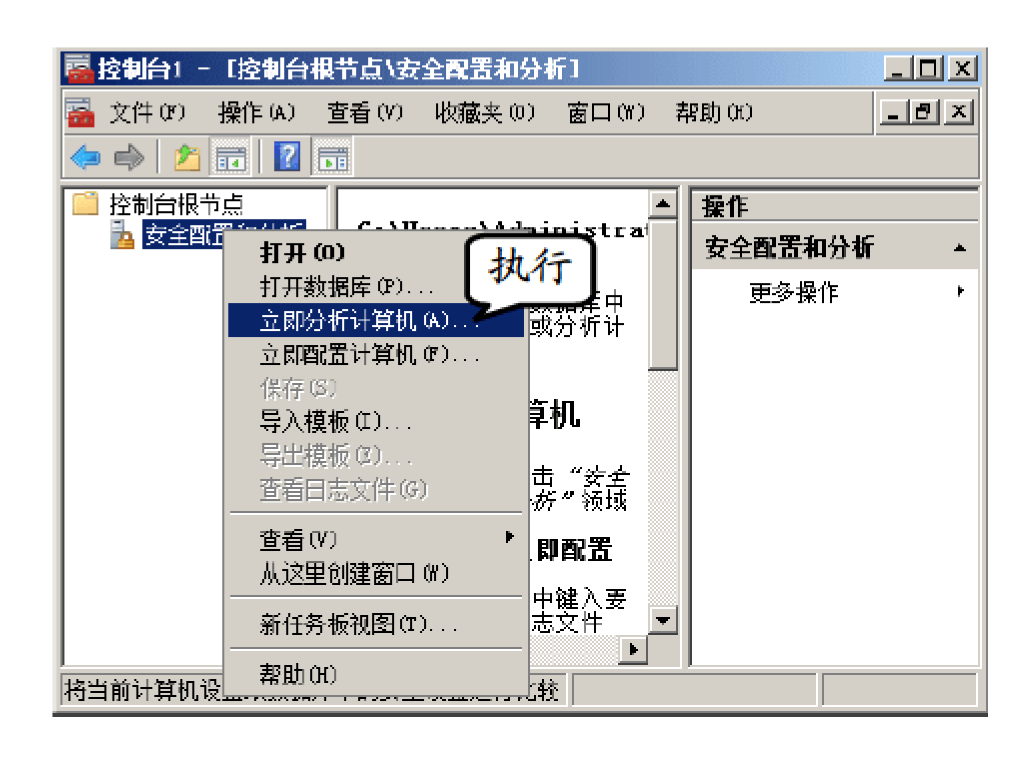


图 5-31　分析计算机

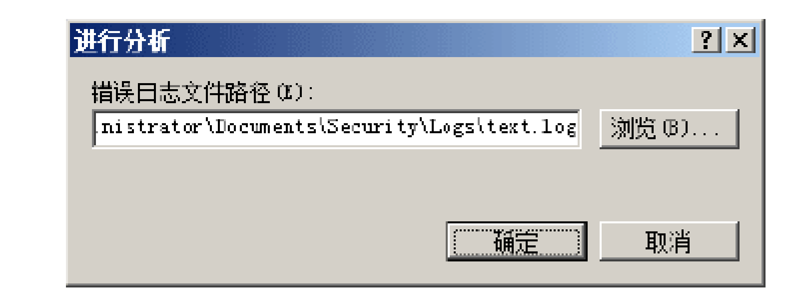


图 5-32　设置文件存放路径

当系统对安全性分析完成后，在控制台中，右击【安全配置和分析】选项，并执行【查看日志文件】命令，即可在控制台右侧的窗口中查看到日志文件的内容，如图 5-33 所示。

4．检测安全性分析结果

通过安全配置和分析工具可以显示安全分析的结果，并使用虚拟标志表明问题。对于安全区域中的每个安全属性，将显示当前系统和基本配置的设置。如果选择接受当前的设置，将修改基本模板中相应的值以与此设置相匹配，如果更改系统设置以匹配基本配置，则当使用安全配置和分析配置系统时，这些更改将会被反映出来。要避免已检查并确定为合理的设置连续标记，可以在模板的副本修改基本设置。

❑ 查看安全性分析结果

在【安全配置和分析】控制台中，依次展开【安全配置和分析】|【账户策略】节点，并单击想要查看的安全策略，如密码策略，如图 5-34 所示。在右侧窗格中，【策略】列表中显示了分析结果；【数据库设置】列表显示模板中的安全值；【计算机设置】列表显示系统中的当前安全策略。



图 5-33　查看日志文件



图 5-34　控制台窗口

另外，还会包括如下的状态标记。

- ❑ “X” 表明与基本配置有差异。
- ❑ “复选标记” 表明与基本配置一致。
- ❑ 没有图标表明模板中不包含安全属性，因此不分析。

例如，【密码必须符合复杂性要求】策略，在安全数据库中的设置为“启用”，而在本地的系统设置为“停用”，分析状态标记为“X”，表示配置不同。而【密码最长存留期】策略在安全数据库中的设置为“42 天”，在本地的系统设置也为“42 天”，分析状态标记为“复选标记”，表示配置相同。

❑ 数据库策略修改

如果网络管理员认为安全数据库的安全策略不符合工作需要，可以更改目前的数据库设置，例如，更改【密码最长使用期限】策略。

在【安全配置和分析】控制台的【密码策略】窗格中，双击【密码最长使用期限】选项，在弹出的对话框中，启用【在数据库中定义这个策略】复选框。然后，在【密码过期时间】文本框中，将原来的 42 天更改为 7 天，如图 5-35 所示。

此时，密码最长存留期策略在安全数据库中的策略为“7 天”，而在本地的系统设置为“42

天”，分析状态标记转变为“X”，表示配置不同，数据库更新成功，如图 5-36 所示。

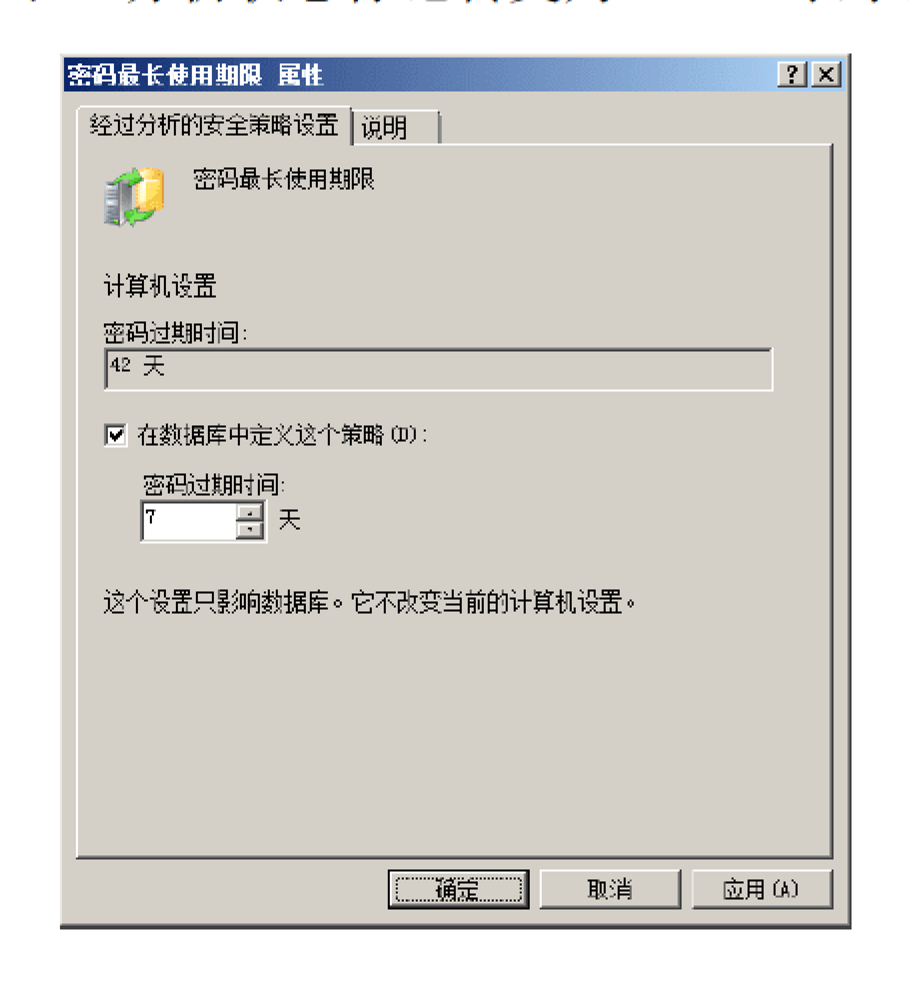


图 5-35 【密码最长使用期限】对话框

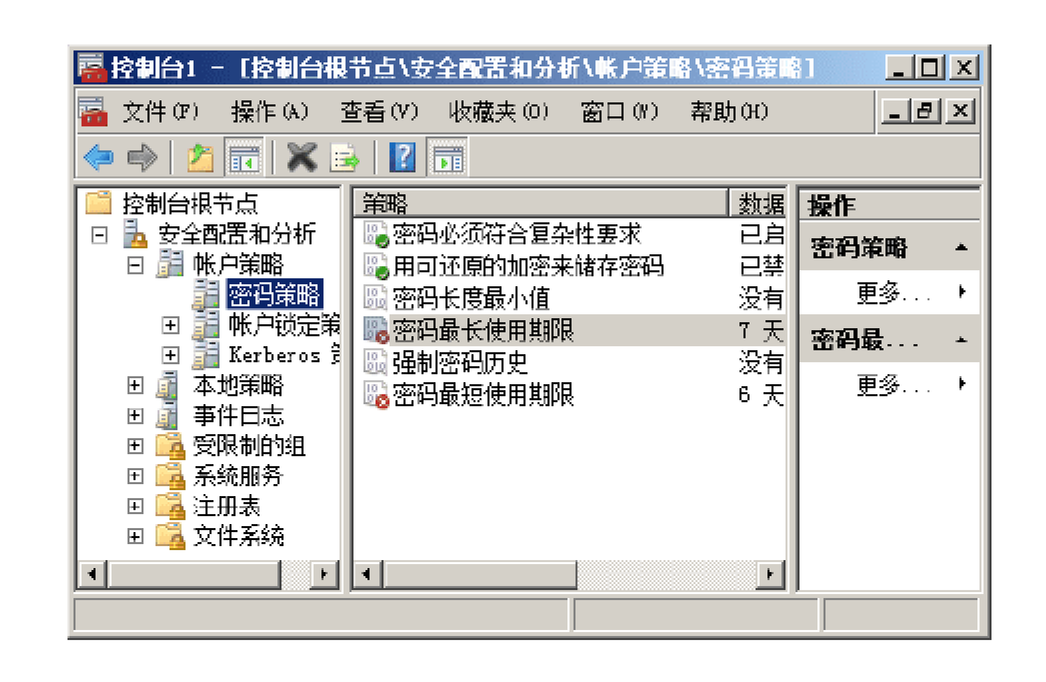


图 5-36 安全数据库更新成功

5. 配置系统安全模板

在分析基于域的用户安全性时，不推荐使用【立即配置系统】选项。在这种情况下，应该返回到【安全模板】管理单元、修改模板，并重新将它应用于适当的“组策略”对象中。

❑ 系统安全模板

无论何时要更改原始安全模板，都必须返回到“安全模板”中。

安全配置和分析工具提供解决显示的任何策略设置值的功能。

如果根据此计算机的环境（角色）确定本地系统的安全级别有效，则接受或更改某些或所有的已标记或不包含在配置中的值。当选择“立即配置系统”时，将更新基本配置中的这些属性值，并将它们应用到系统。

如果确定系统不符合有效的安全级别，则将系统配置为原始基本配置值。

根据计算机的角色，将更适合的模板导入到数据库中作为新的基本配置，并把它应用于系统中。

对存储在数据库中的模板进行更改，而不是对安全模板文件。如果返回到安全模板中并编辑此模板或将存储的配置导出到相同的模板文件中时，才会修改安全模板。

❑ 安全模板应用

在【安全配置和分析】控制台中，设置工作数据库（如果当前没有设置工作数据库，该步骤是必须的）。

右击【安全配置和分析】选项，执行【立即配置系统】命令，在弹出的对话框中提示设置分析日志存储位置，通常可以选择使用默认的错误文件路径，单击【确定】按钮即可，如图 5-37 所示。当然，也可以输入新的日志的文件名和有效路径。当系统配置完成后，就可以检查日志文件或复查结果。

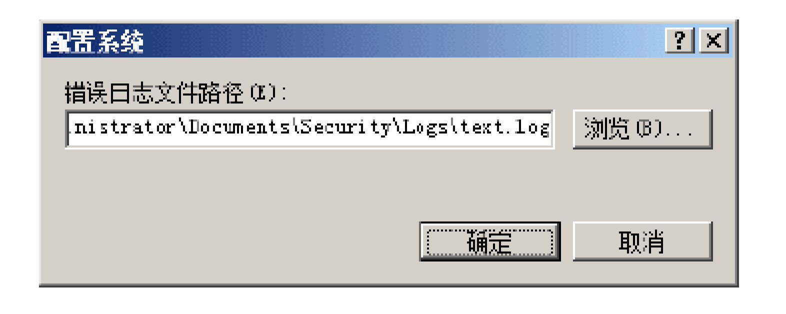


图 5-37 【配置系统】对话框

5.4.4 网管心得——企业系统监控安全策略

尽管不断地对系统进行修补，但由于软件系统的复杂性，新的安全漏洞总会层出不穷。因此，除了对安全漏洞进行修补之外，还要对系统的运行状态进行实时监控，以便及时发现利用各种漏洞的入侵行为。如果已有安全漏洞但还没有全部得到修补时，这种监控就显得尤其重要。

1. 启用系统审核机制

系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员进行分析、查找系统和应用程序故障以及各类安全事件。

所有的操作系统、应用系统等都带有日志功能，因此可以根据需要实时地将发生在系统中的事件记录下来。同时还可以通过查看与安全相关的日志文件的内容来发现黑客的入侵和入侵后的行为。

2. 日志监视

在系统中启用安全审核策略后，管理员应经常查看安全日志的记录，否则就失去了及时补救和防御的时机了。除安全日志外，管理员还要注意检查各种服务或应用的日志文件。在 Windows 2008 IIS 7.0 中，其日志功能默认已经启动，并且日志文件存放的路径默认在 System32/LogFiles 目录下，打开 IIS 日志文件，可以看到对 Web 服务器的 HTTP 请求，IIS 7.0 系统自带的日志功能从某种程度上可以成为入侵检测的得力帮手。

3. 监视开放的端口和连接

对日志的检查只能发现已经发生的入侵事件，但是对正在进行的入侵和破坏行为无能为力。这时就需要管理员掌握一些基本的实时监视技术。

通常在系统被黑客或病毒入侵后，就会在系统中留下木马类后门。同时它和外界的通信会建立一个 Socket 会话连接，这样就可能发现它，netstat 命令可以进行会话状态的检查，在这里就可以查看已经打开的端口和已经建立的连接。当然也可以采用一些专用的检测程序对端口和连接进行检测。

4. 监视共享

通过共享入侵一个系统是最常见的一种方法。如果防范不严，最简单的方法就是利用系统隐含的管理共享。因此，只要黑客能够扫描到 IP 地址和用户密码，就可以使用 net use 命令连接到共享上。另外，当浏览含有恶意脚本的网页时，此时计算机的硬盘也可能被共享，因此，监测本机的共享连接是非常重要的。

5. 监视进程和系统信息

对于木马和远程监控程序，除监视开放的端口外，还应通过任务管理器的进程查看功能进行进程的查找。通常，隐藏的进程寄宿在其他进程下，因此查看进程的内存映象也许能发

现异常。现在的木马越来越难发现，它常常会把自己注册成为一个服务，从而避免在进程列表中现形。因此，应结合对系统中的其他信息的监视，这样就可对系统信息中的软件环境下的各项进行相应的检查。

5.5　IPSec 安全策略

IPSec（Internet Protocol Security，Internet 协议安全）策略是 Windows Server 2008 中自带的 IP 安全策略设置组件，通过它可以针对网络数据的源 IP 地址、目的 IP 地址以及使用的协议、端口等信息进行详细的设置，可以管理进程计算机的网络数据包。也就是说，IPSec 具有类似于路由交换设备中的访问控制列表功能，控制着数据的访问权限。

IPSec 是解决网络安全问题的重要手段，可以为专用网络和 Internet 建立重要的安全防线，并使得网络安全性和易用性之间取得平衡。IPSec 是一种加密的标准，它允许在差别很大的设备之间进行安全通信。利用 IPSec 不仅可以构建基于操作系统的防火墙，实现一般防火墙的功能，还可以为许可通信的 2 个端点建立加密的、可靠的数据通道。

5.5.1　IPSec 服务

在 Windows Server 2008 安装完成后，IPSec 默认以服务的方式存在，但未被启用，需要管理员手动启用该服务。

如果需要查看并启用 IPSec 服务，首先需要执行【开始】|【运行】命令，在弹出的对话框中，输入 services.msc 命令，并单击【确定】按钮。然后，在【服务】窗口中右击 IPsec Policy Agent 选项，并执行【属性】命令，如图 5-38 所示。

在弹出的对话框中，设置该服务的启动类型为“自动（延时启动）”，并单击【应用】按钮，然后，单击【启动】按钮，启动该服务，如图 5-39 所示。

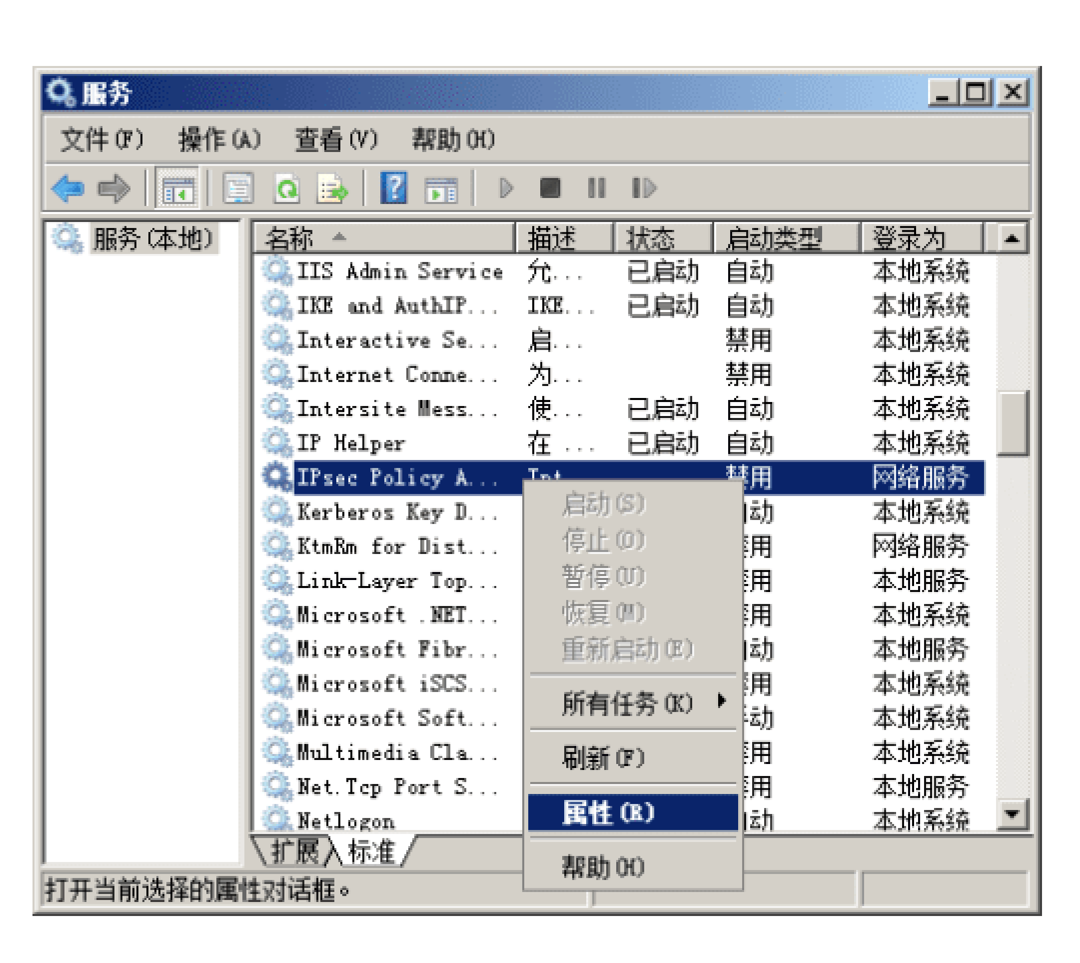


图 5-38　【服务】窗口



图 5-39　启动 IPSec 服务

5.5.2 创建 IPSec 连接安全规则

IPSec 连接安全规则允许用户为满足指定标准的联机请求 IPSec，这些标准类似于 Windows 防火墙筛选器。例如，用户可以为如下情况设置 IPSec 安全规则。

- ❑ 拒绝来自指定 IP 地址的所有通信。
- ❑ 拒绝所有来自默认网关的 ICMP 通信。
- ❑ 拒绝所有来自内网的发往指定端口的通信。
- ❑ 限制除了特定服务器的所有出站连接。

在网络中，每一台计算机只能拥有一个 IPSec 策略。如果多个策略应用于同一台计算机，每个组策略都有不同的 IPSec 策略，那么只有最高级的 IPSec 策略会起作用。

如果要创建 IPSec 策略，首先需要执行【开始】|【管理工具】|【高级安全 Windows 防火墙】命令，在打开的窗口中，选择【连接安全规则】选项。然后，在右侧【操作】窗格中，单击【新规则】选项，如图 5-40 所示。

在【规则类型】对话框中，选中【自定义】单选按钮，并单击【下一步】按钮，如图 5-41 所示。对于该对话框中的其他选项有如下说明。



图 5-40 【高级安全 Windows 防火墙】窗口



图 5-41 选择规则类型

- ❑ **隔离** 可根据用户定义的身份验证标准对连接进行限制。例如，可以使用该规则类型，隔离域中的计算机和域外的计算机。
- ❑ **身份验证例外** 可以使用该规则类型，使特定的计算机或者指定范围内的 IP 地址（计算机），免于对自身进行身份验证，而不考虑其他连接安全规则。
- ❑ **服务器到服务器** 使用此规则类型对两台特定计算机之间、两个计算机组之间、两个子网之间或者特定计算机和计算机组或子网之间的通信，进行身份验证。
- ❑ **隧道** 如果在不知 IPSec 的网络中，为支持 IPSec 的客户端和服务器创建 IPSec 连接安全规则，则必须使用隧道模式。

- 自定义　使用该规则类型创建需要特殊设置的规则。

在【终结点】对话框中，选中【终结点 1 中的计算机】区域内的【下列 IP 地址】单选按钮，单击【添加】按钮。然后，在弹出的【IP 地址】对话框中的【此 IP 地址或子网】文本框中输入添加的 IP 地址，并单击【确定】按钮，如图 5-42 所示。

在接下来弹出的对话框中，保持默认设置，依次单击【下一步】按钮即可，直到在弹出的【名称】对话框中的【名称】文本框内，输入该规则的名称以及在【描述（可选）】文本框内输入对该规则的描述信息。然后，单击【完成】按钮，如图 5-43 所示。

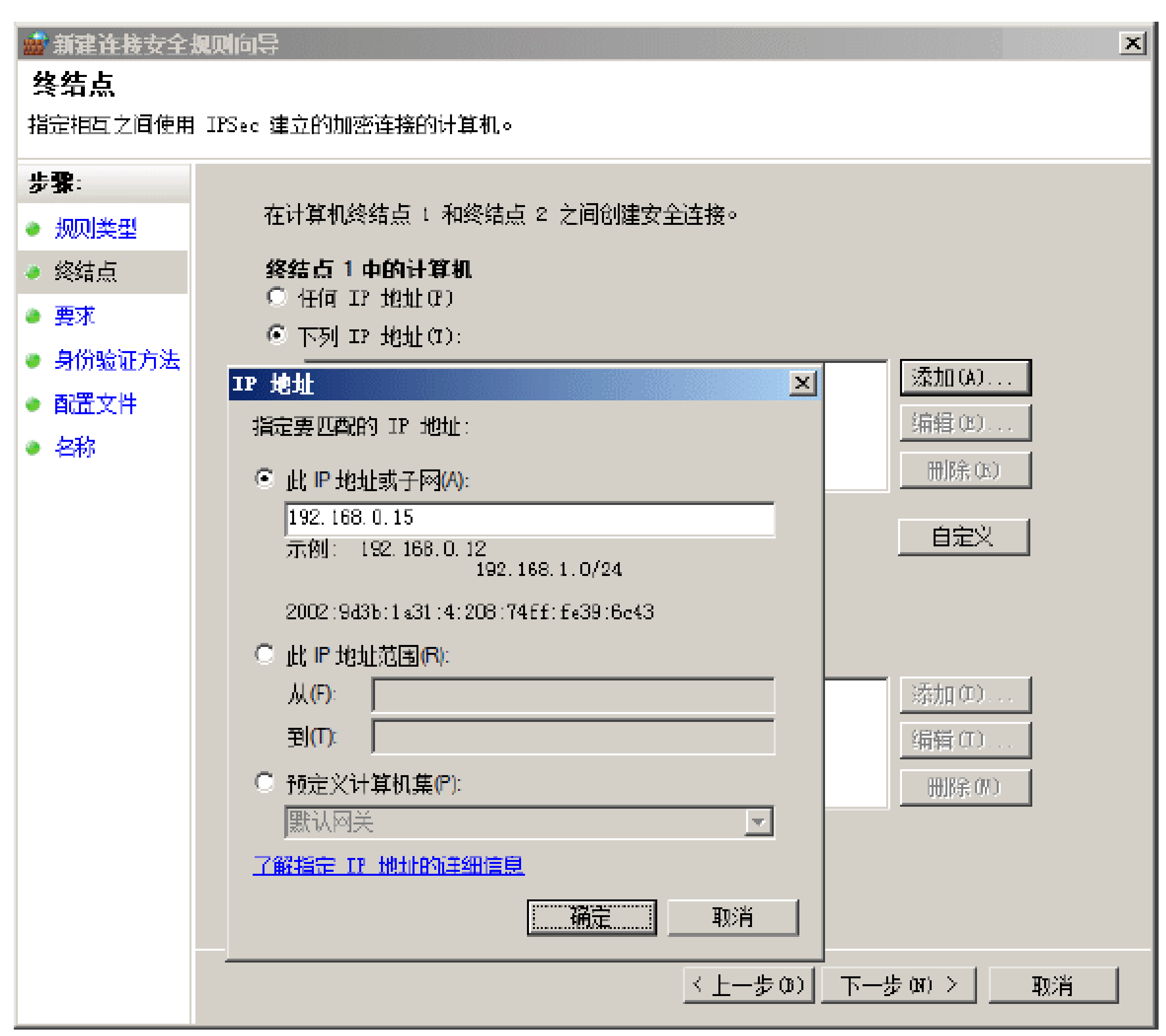


图 5-42　设置终结点

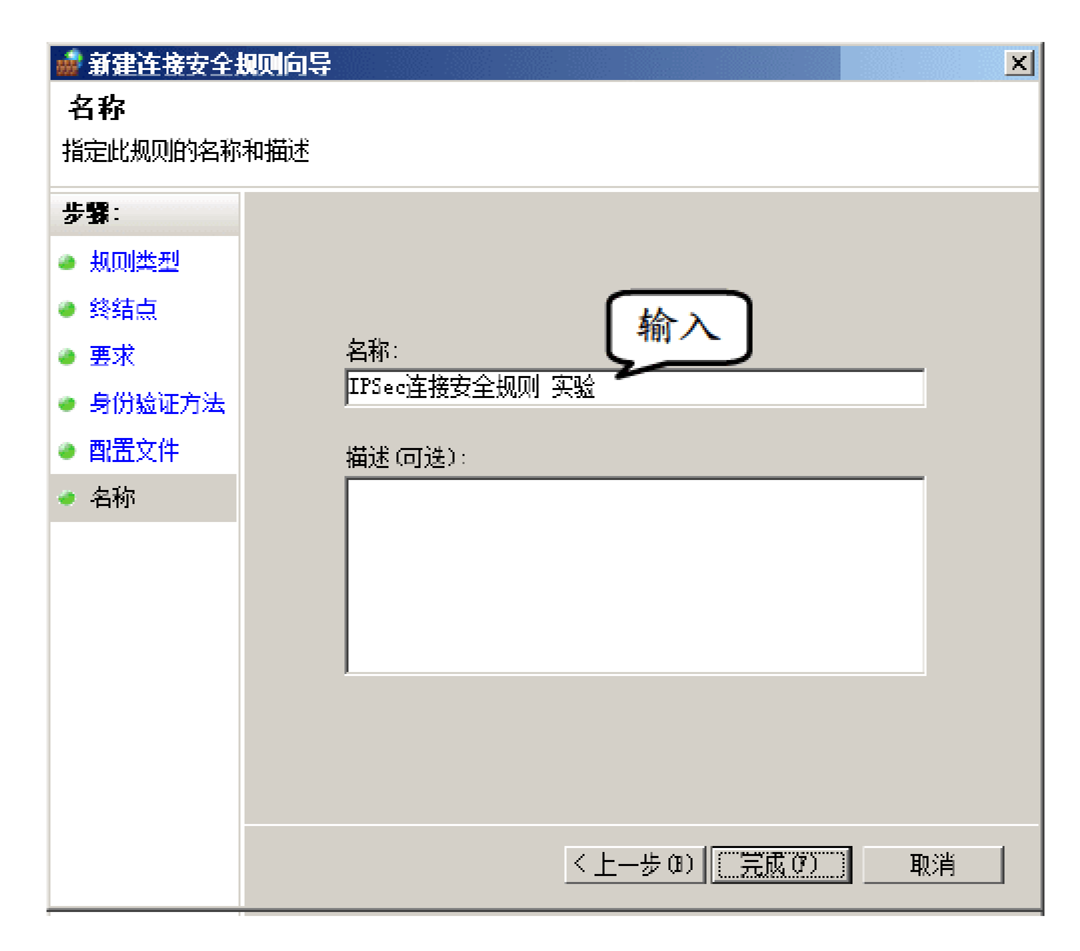


图 5-43　创建规则完成

5.6　操作实例

5.6.1　操作实例——限制外部链接

在网络中，若系统账户没有做任何策略，入侵者只要具有足够的耐心，通过使用自动登录及密码猜解字典工具进行攻击，那么破解密码只是一个时间和运气上的问题。为了避免这种情况的发生，就要设置相应的安全策略，以限制外部链接，保证网络及系统的安全。

1．实例目的

- 应用各种策略。
- 防范各种攻击。
- 保障系统安全。

2．实例步骤

（1）在桌面单击【开始】菜单，执行【程序】|【管理工具】|【本地安全策略】命令，在

弹出的窗口中，展开【账户策略】节点，选择【密码策略】选项。然后，双击【密码必须符合复杂性要求】策略，如图 5-44 所示。

（2）在弹出的对话框中，选中【已启用】单选按钮，并单击【确定】按钮，如图 5-45 所示。

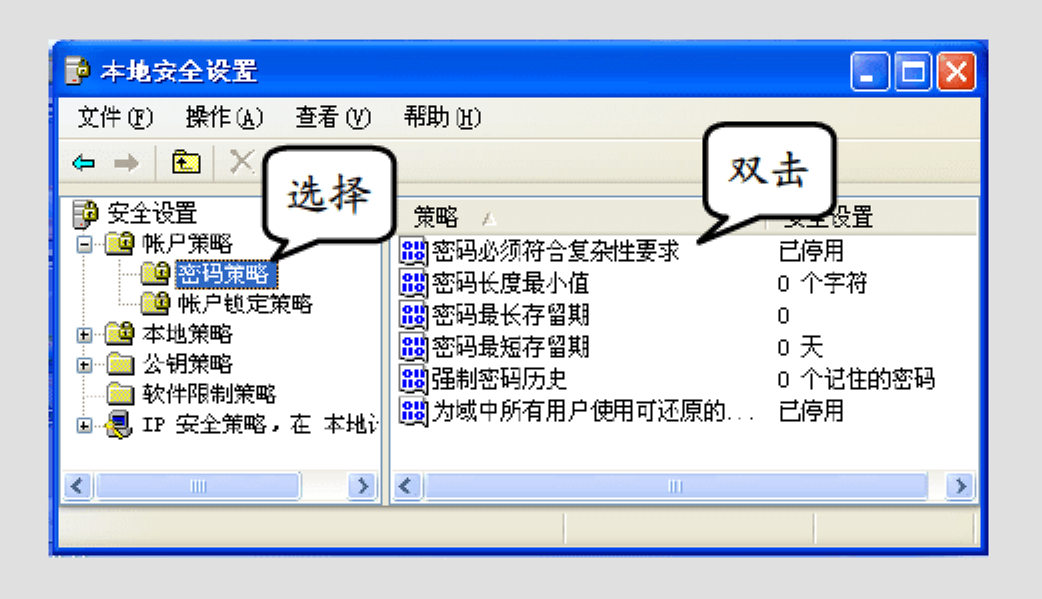


图 5-44 选择密码策略

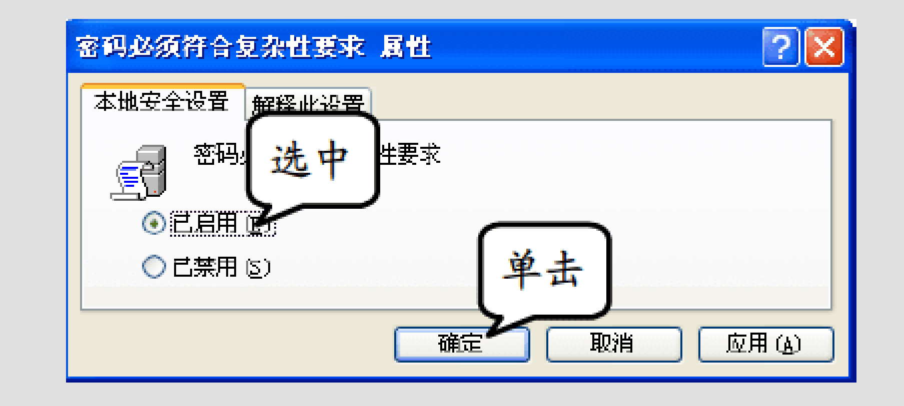


图 5-45 启用该策略

（3）在【密码策略】中，双击【密码长度最小值】策略，在弹出的对话框的文本框中输入数字“8”，并单击【确定】按钮，如图 5-46 所示。



密码至少是 8 个字符，最长为 14 个字符，字符数设置为 0 时，表示不需要密码。在域控制器上的默认值为 7，而在独立服务器上为 0。

（4）在【密码策略】中，双击【密码最长存留期】策略，在弹出对话框的文本框中输入“7”，并单击【确定】按钮，如图 5-47 所示。

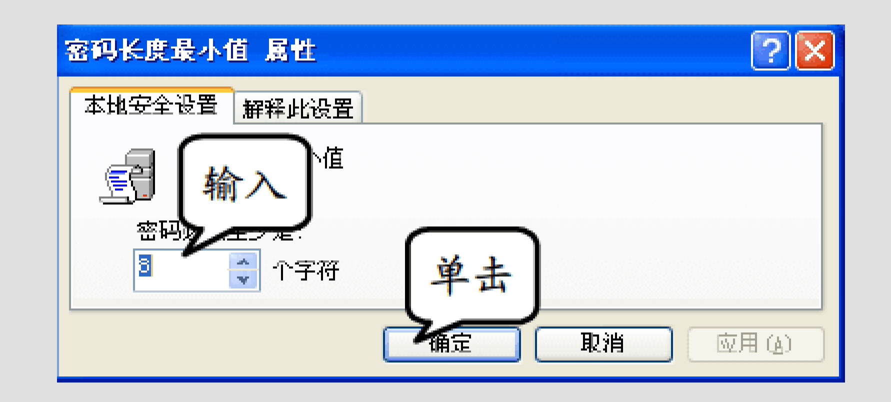


图 5-46 设置最小密码长度

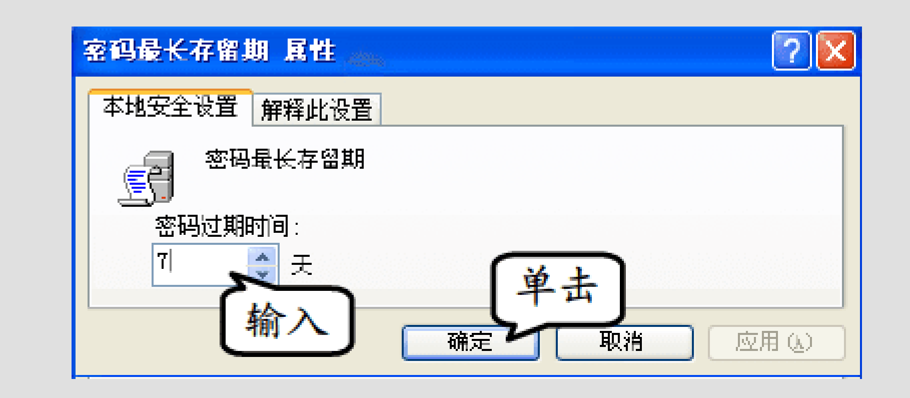


图 5-47 设置密码过期时间

（5）在【本地安全设置】主窗口中，选择【账户锁定策略】，并双击【账户锁定阈值】策略，如图 5-48 所示。

（6）在弹出的对话框的文本框中输入“3”，并单击【确定】按钮，如图 5-49 所示。

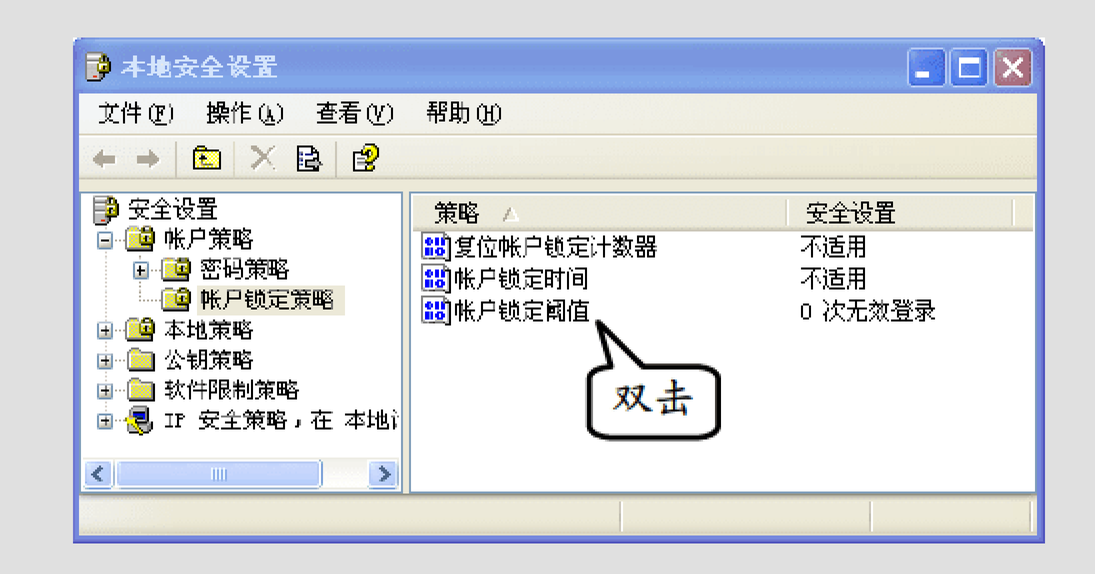


图 5-48 双击账户锁定阈值

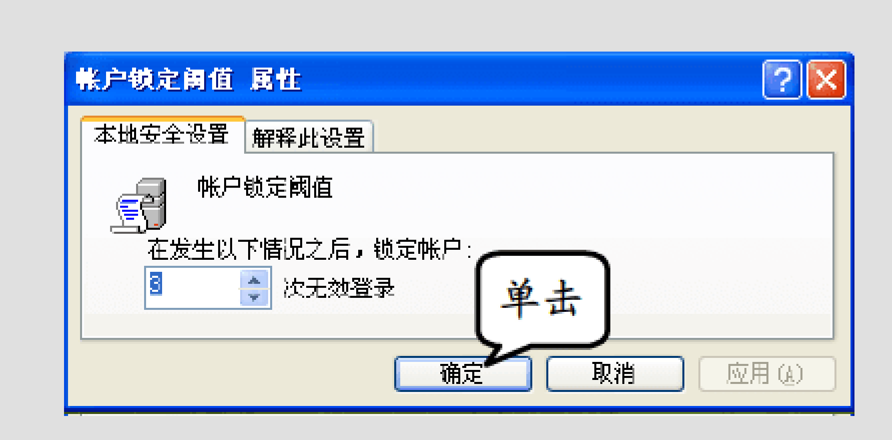


图 5-49 设置锁定账户阈值



在 3 次无效登录后，用户将被锁定。这个数值介于 0 到 999 之间，如果将值设置为 0，则永远不会锁定账户。

（7）在弹出的对话框中，单击【确定】按钮，如图 5-50 所示。

（8）执行【开始】|【运行】命令，在弹出的对框内输入 cmd 命令，并单击【确定】按钮。在弹出的命令提示符窗口中输入 net user shenglin !!shenglin /add 和 net user shenglin !!sheng951 /add 命令后分别按回车键，如图 5-51 所示。

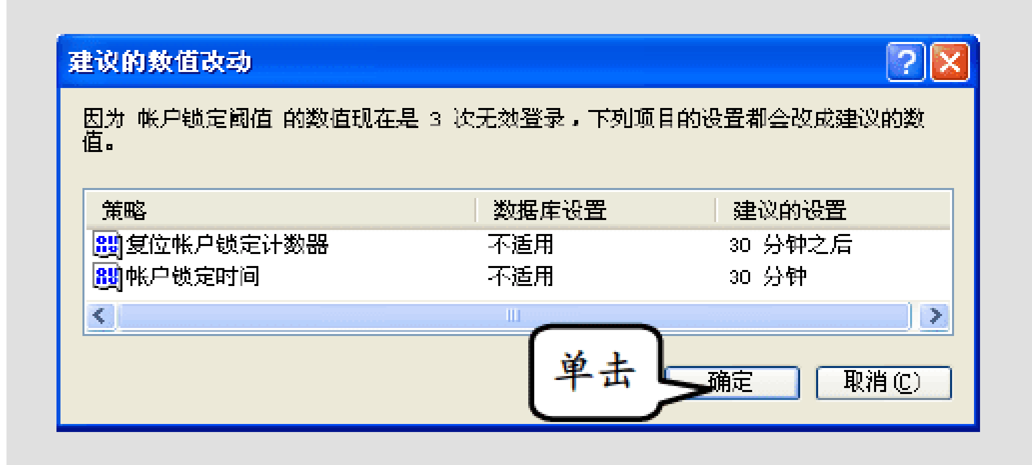


图 5-50　默认其他设置

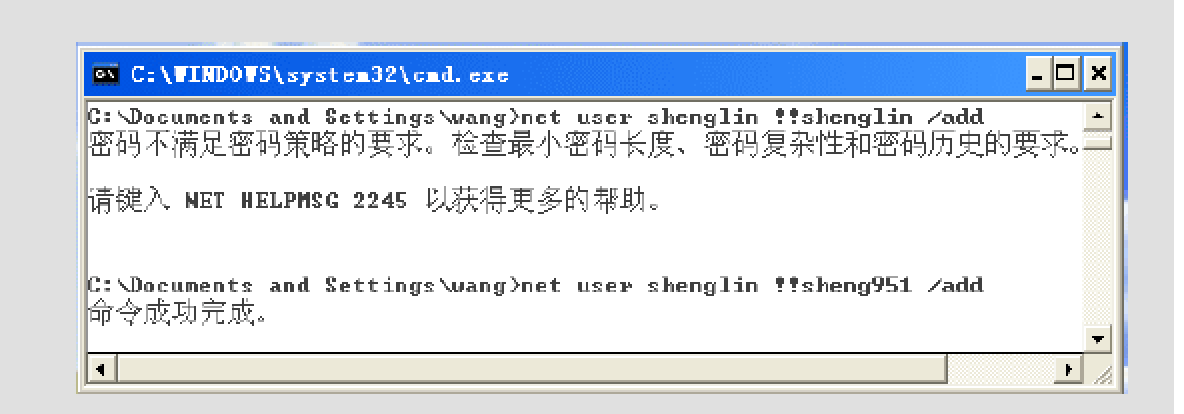


图 5-51　验证策略是否生效



第 1 个命令的意思：建立用户 shenglin，并设立密码为!! shenglin，结果是不能够完成执行命令。第二个命令的意思：建立用户 shenglin 并设立密码为!!shenglin951，结果是能够成功执行命令。原因：第 1 个命令不符合密码复杂性的策略要求，而第 2 个符合。

（9）在【登录到 Windows】对话框的【用户名】和【密码】文本框中，输入用户名和密码（输入 3 次错误的密码），并单击【确定】按钮，如图 5-52 所示。

（10）在该对话框中，再次输入相应的用户名和密码（输入正确的用户名和密码），并单击【确定】按钮。然后，在弹出的对话框中，单击【确定】按钮，如图 5-53 所示。



图 5-52　验证策略是否生效

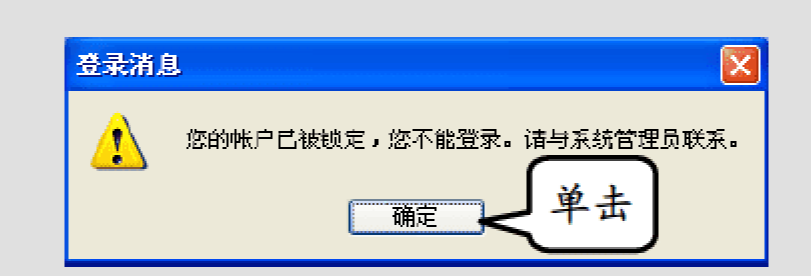
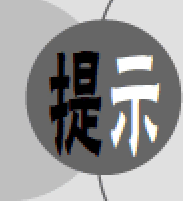


图 5-53　账户被锁定，策略生效



在 3 次无效登录后，该用户账户即被锁定，即使输入正确的用户名和密码，也不能够登录系统。因此，验证了本地安全策略能够防范他人通过自动登录工具和密码猜解字典进行攻击，从而起到限制外部链接的作用。

5.6.2 操作实例——防范网络嗅探

由于局域网采用广播的方式进行通信，因而信息很容易被窃听。网络嗅探就是通过侦听所在网络中所传输的数据来嗅探有价值的信息。对于普通的网络嗅探的防御并不困难，可以采用 IPSec 安全策略（启到加密通信数据的作用）。

1. 实例目的

- ❑ 开启审核策略。
- ❑ 激活 IPSec。
- ❑ 验证 IPSec 建立。

2. 实例步骤

（1）在一个网络中，有一台安全服务器和一台客户端，其 IP 分别是“192.168.1.1”和“192.168.1.2”，拓扑结构如图 5-54 所示。

（2）在安全服务器中，单击【开始】菜单，执行【程序】|【管理工具】|【本地安全策略】命令，在打开的窗口中，展开【本地策略】节点，单击【审核策略】选项。然后，在右侧的窗格中双击【审核登录事件】策略，如图 5-55 所示。

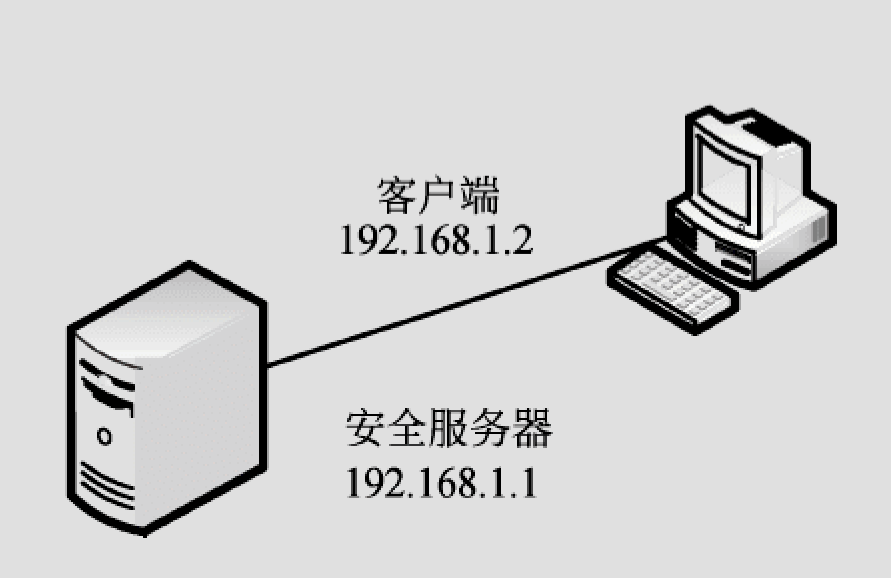


图 5-54 拓扑结构示意图

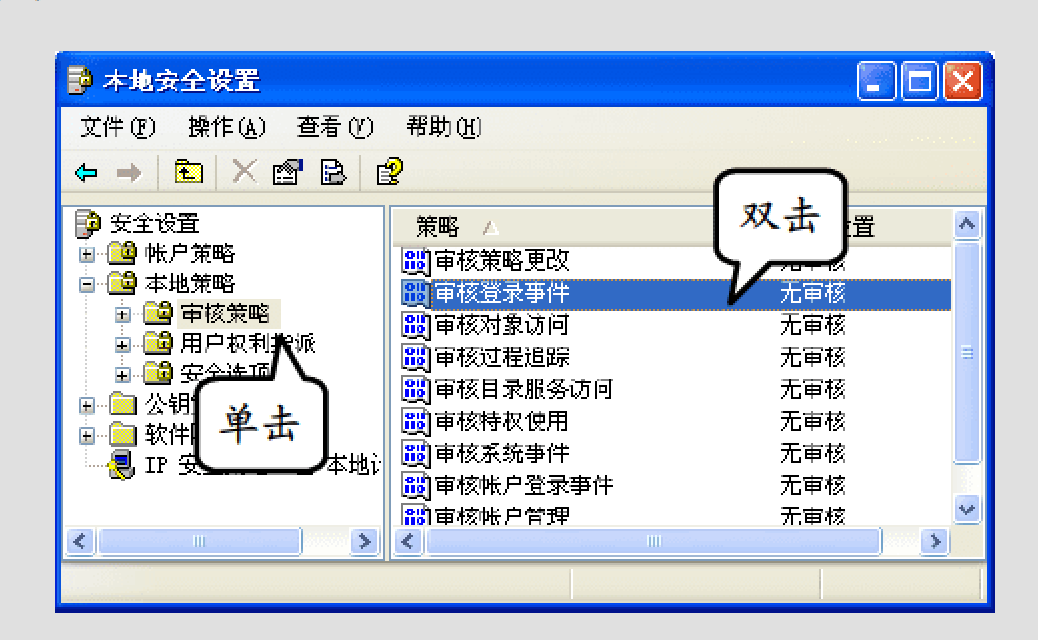


图 5-55 本地安全设置

（3）在弹出的对话框中，启用【成功】和【失败】复选框，并依次单击【应用】和【确定】按钮，如图 5-56 所示。



提示：不论用户登录成功或失败，都会被记录在安全日志内。

（4）在【审核策略】选项中，双击【审核对象访问】策略，在弹出的对话框中，启用【成功】和【失败】复选框，并依次单击【应用】和【确定】按钮，如图 5-57 所示。



提示：其他用户访问本地计算机时，不论成功或失败都会被记录在系统日志中。

（5）在【本地安全设置】窗口中，选择【IP 安全策略，在 本地计算机】选项，在右侧的

窗格中，双击【安全服务器（需要安全）】策略，如图 5-58 所示。

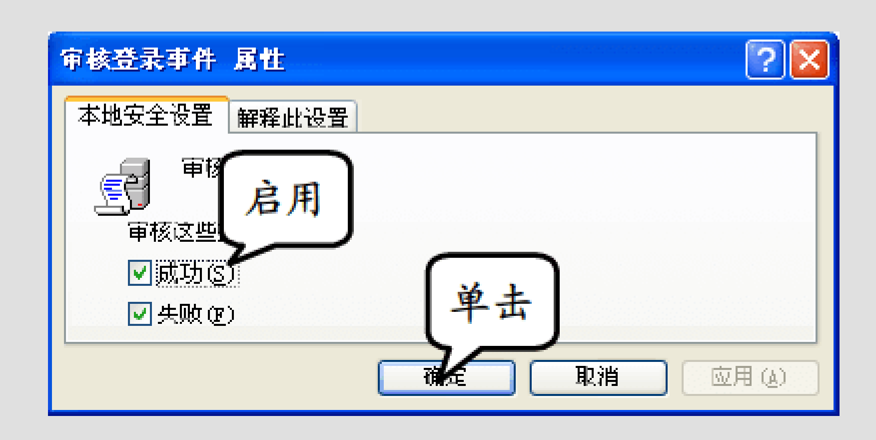


图 5-56 应用该策略

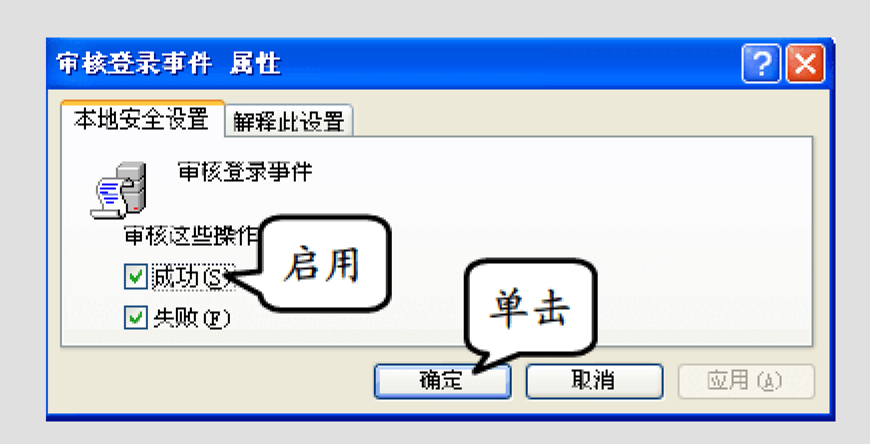


图 5-57 审核账户登录事件

（6）在弹出的对话框中，双击【所有 IP 通讯量】选项，如图 5-59 所示。

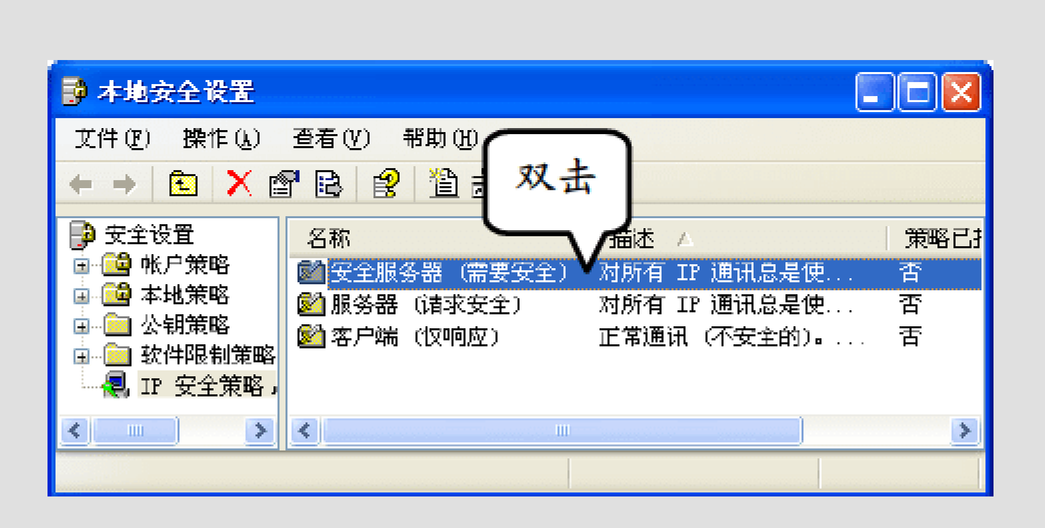


图 5-58 本地安全设置

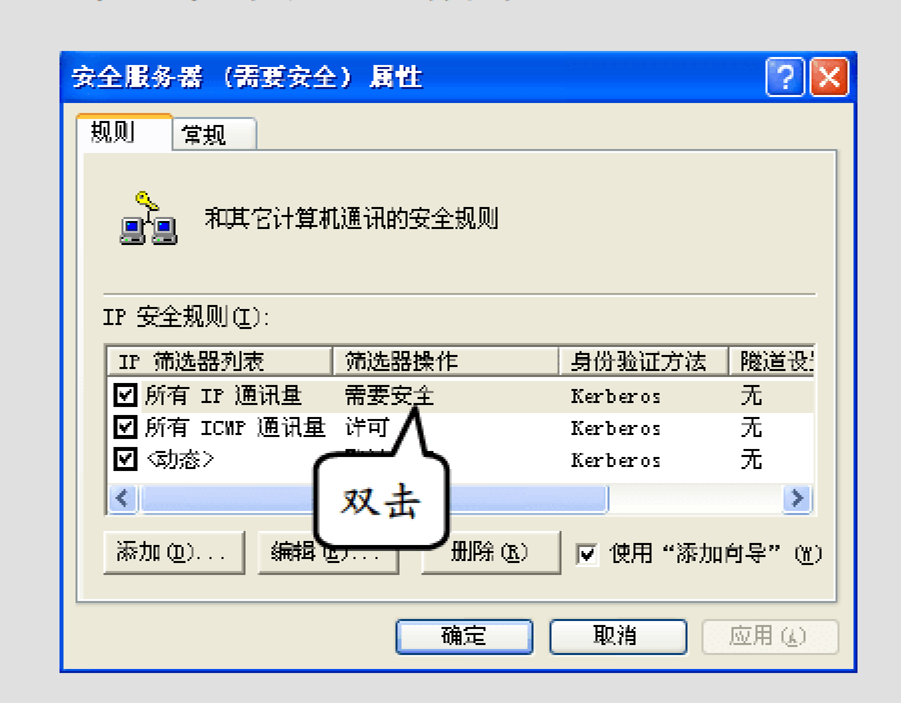


图 5-59 修改默认配置

（7）在【编辑规则 属性】对话框中，选择【身份验证方法】选项卡，并单击【添加】按钮，如图 5-60 所示。

（8）在弹出的对话框中，选中【使用此字符串（预共享密钥）】单选按钮，并在下方的文本框中输入“123456”字符串。然后，单击【确定】按钮，如图 5-61 所示。

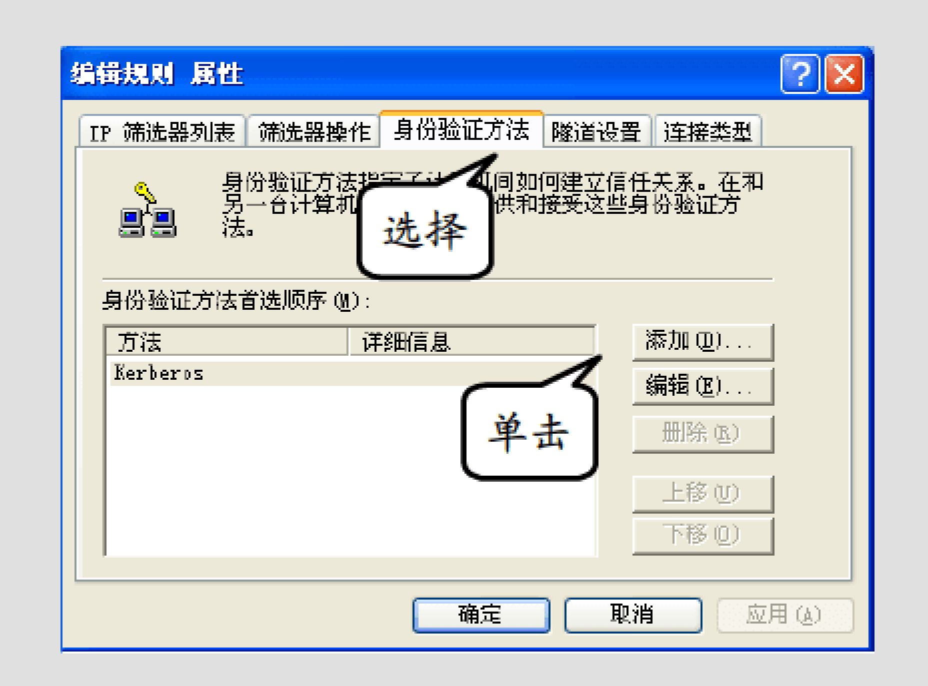


图 5-60 添加身份验证方法

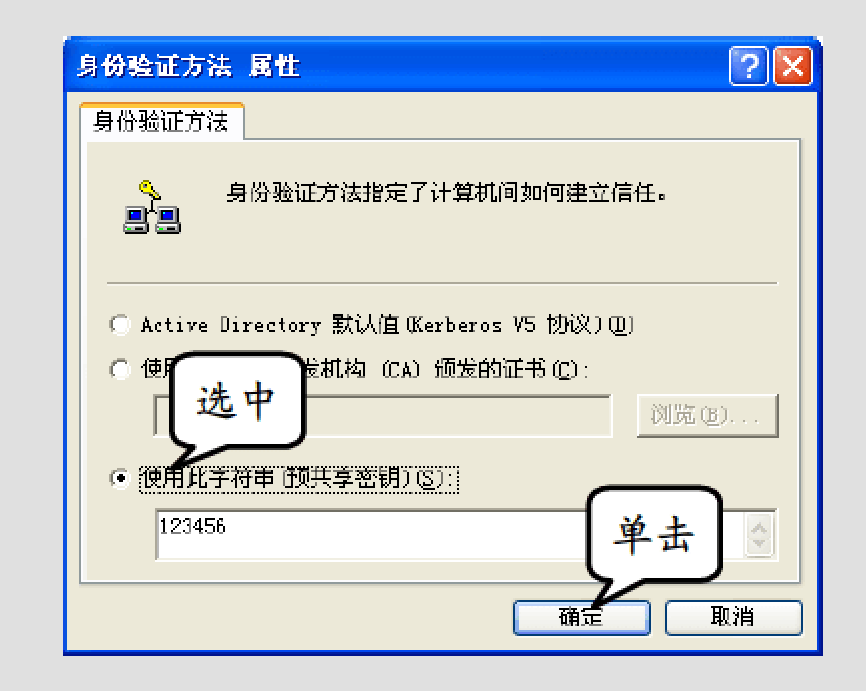


图 5-61 添加预共享密钥



预共享密钥字符串可以随意定义，但是相互通信的计算机的预共享密钥必须一致。

（9）在【编辑规则 属性】对话框中，依次单击【应用】和【确定】按钮，如图 5-62 所示。



Kerberos 身份验证方法不能在 Windows XP 系统内使用，因此使用预共享密钥身份验证方法。

（10）使用同样的方法，更改【所有 ICMP 通讯量】和【动态】的身份验证方法，单击【确定】按钮，如图 5-63 所示。

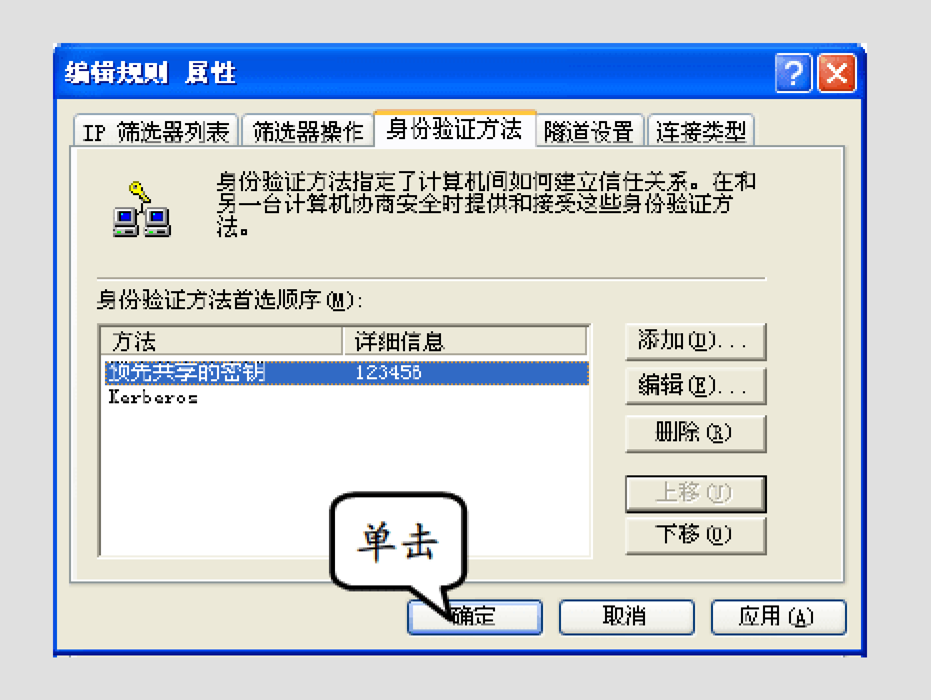


图 5-62　应用预共享密钥

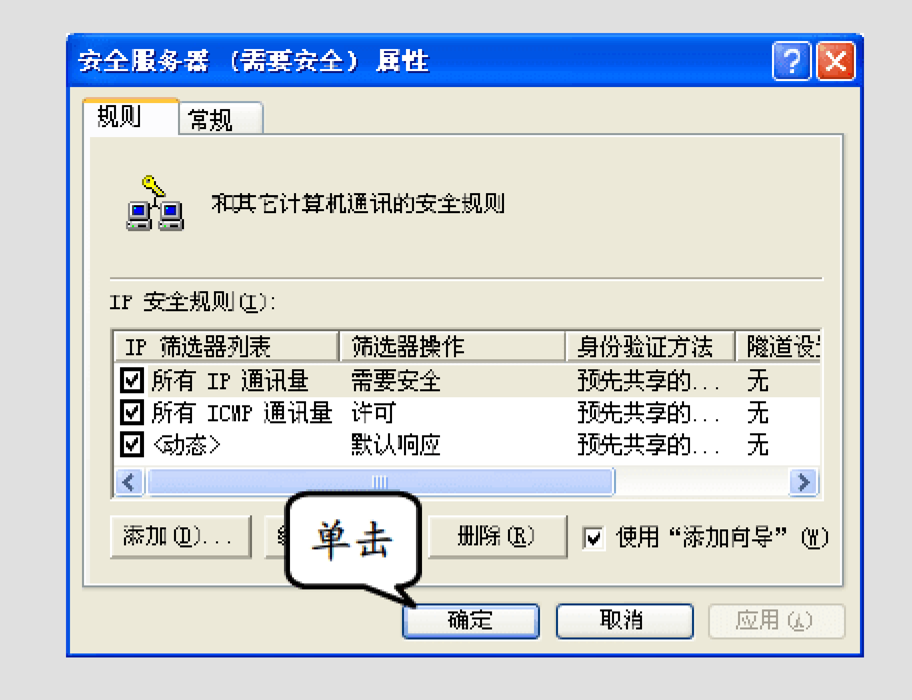


图 5-63　修改完成

（11）在【本地安全设置】窗口中，右击【安全服务器（需要安全）】选项，并执行【指派】命令，如图 5-64 所示。

（12）在客户机桌面中，如第（2）步所示，打开【本地安全设置】窗口，选择【IP 安全策略，在 本地计算机】选项，并双击【客户端（仅响应）】策略，按如上步骤添加并修改身份验证方法，依次单击【应用】和【确定】按钮，如图 5-65 所示。

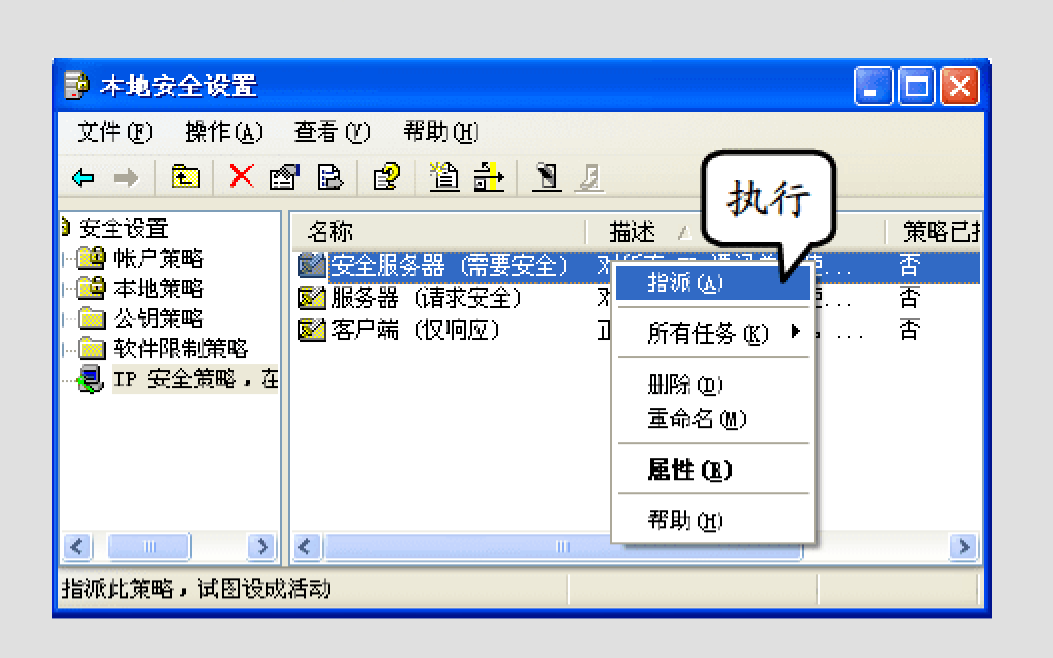


图 5-64　激活安全服务器端 IPSec

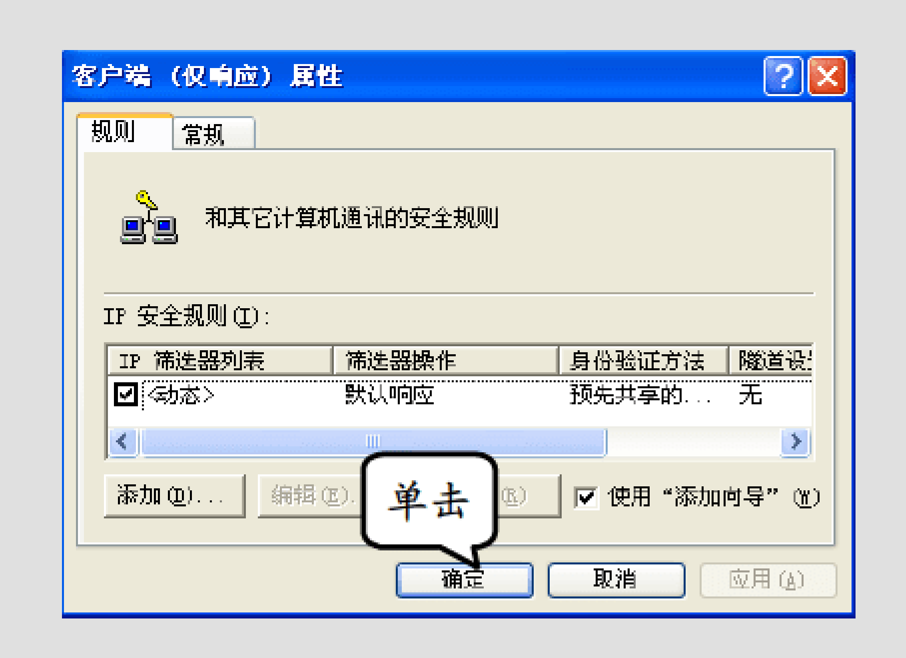


图 5-65　应用预共享密钥

（13）在【本地安全设置】窗口的右侧窗格中，右击【客户端（仅响应）】选项，并执行【指派】命令，如图 5-66 所示。

（14）执行【开始】|【运行】命令，在弹出的对框内输入 cmd 命令，并单击【确定】按钮。在弹出的【命令提示符】窗口中输入 ping 192.168.1.1 命令，按回车键，如图 5-67 所示。

（15）执行【开始】|【程序】|【管理工具】|【事件查看器】命令，在打开的窗口中，展开【事件查看器】节点，选择【安全性】选项。在右侧的窗格中，逐个双击【成功审核】事件，如图 5-68 所示。

（16）在【事件 属性】对话框中，用户可以查看到【描述】文本框内的内容，如图 5-69 所示。

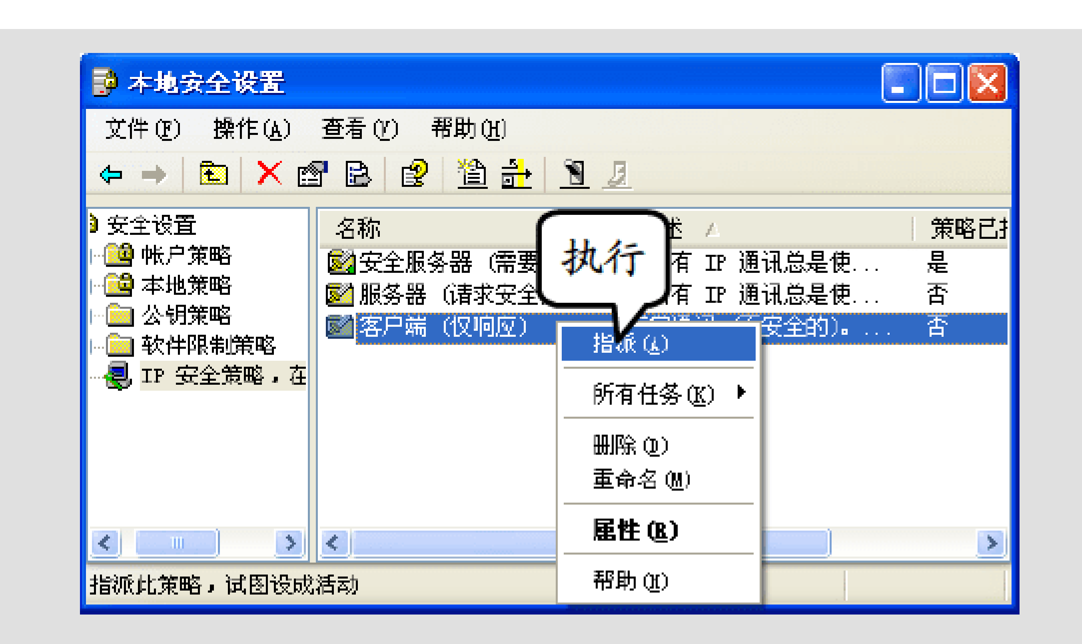


图 5-66　激活客户端 IPSec

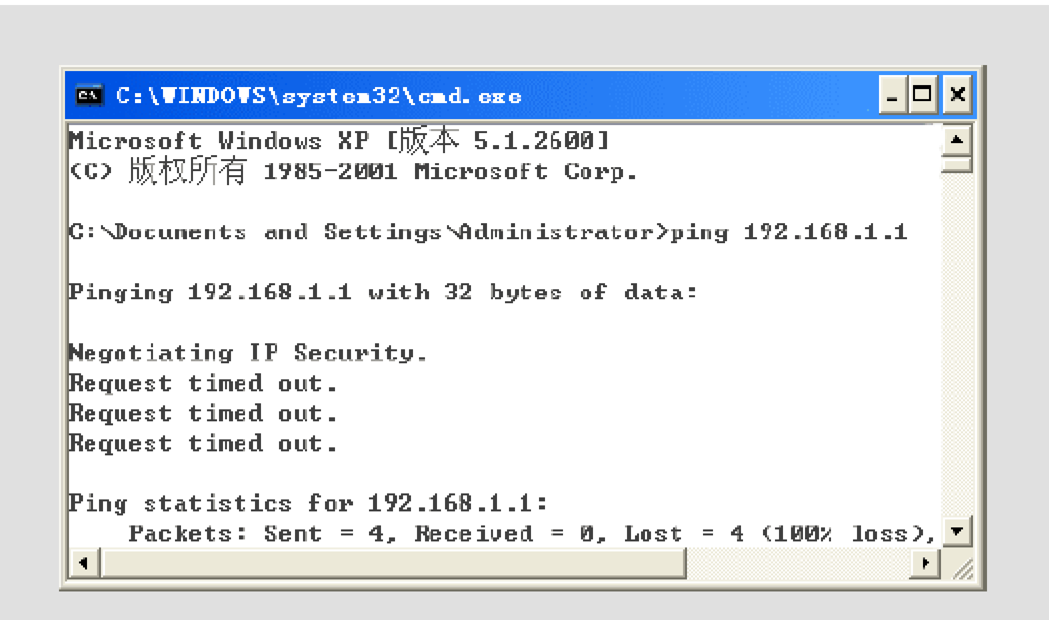


图 5-67　ping 命令

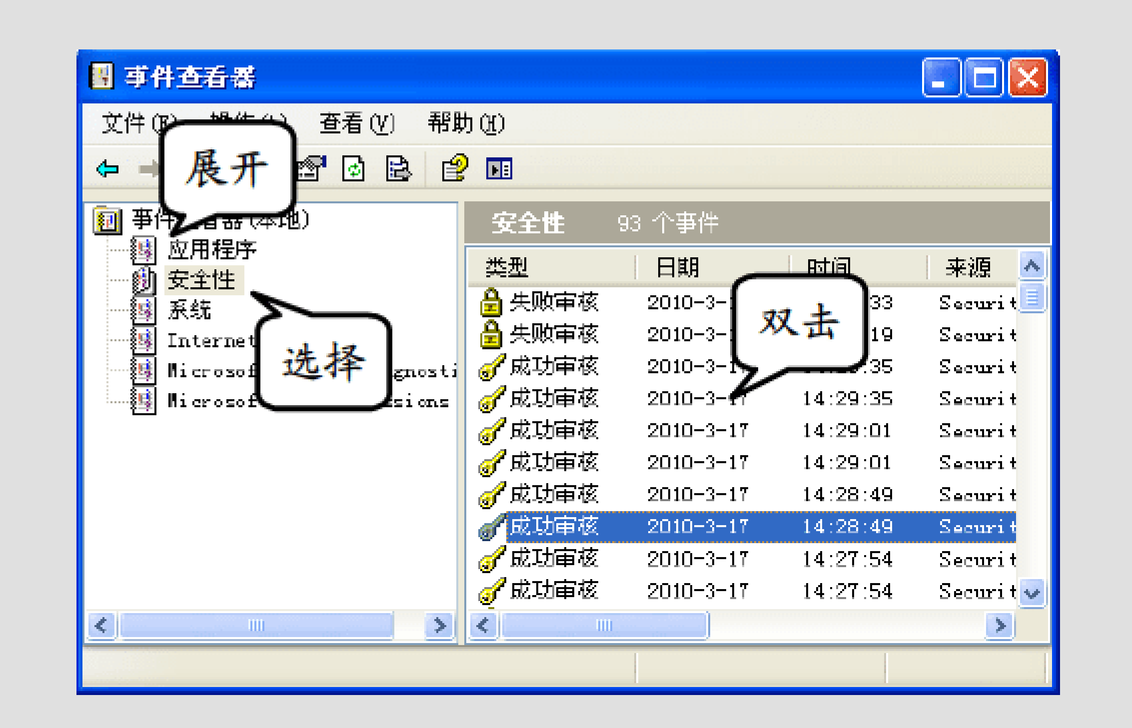


图 5-68　查看安全日志



图 5-69　IKE 安全关联成功建立



IKE 安全关联成功建立后，安全服务器和客户机通信时，使用嗅探工具截获的都是经过加密的数据。因此，可以防范网络嗅探。

5.6.3　操作实例——限制特权组成员

在单位或公司网络中，通过限制特权组成员，能够降低恶意软件及用户意外错误配置所带来的安全风险。同时，也增强了系统的安全性及可管理性。

1．实例目的

- ❑ 限制特权组成员。
- ❑ 保障系统安全。

2．实例步骤

（1）在桌面执行【开始】|【运行】命令，在弹出的对话框中输入 mmc 命令，并单击【确定】按钮。在打开的窗口中，单击【文件】菜单，执行【添加/删除管理单元】命令，如图 5-70

所示。

（2）在弹出的对话框中，单击【添加】按钮，在【可用的独立管理单元】列表中，选择【安全模板】选项，依次单击【添加】和【关闭】按钮，如图 5-71 所示。

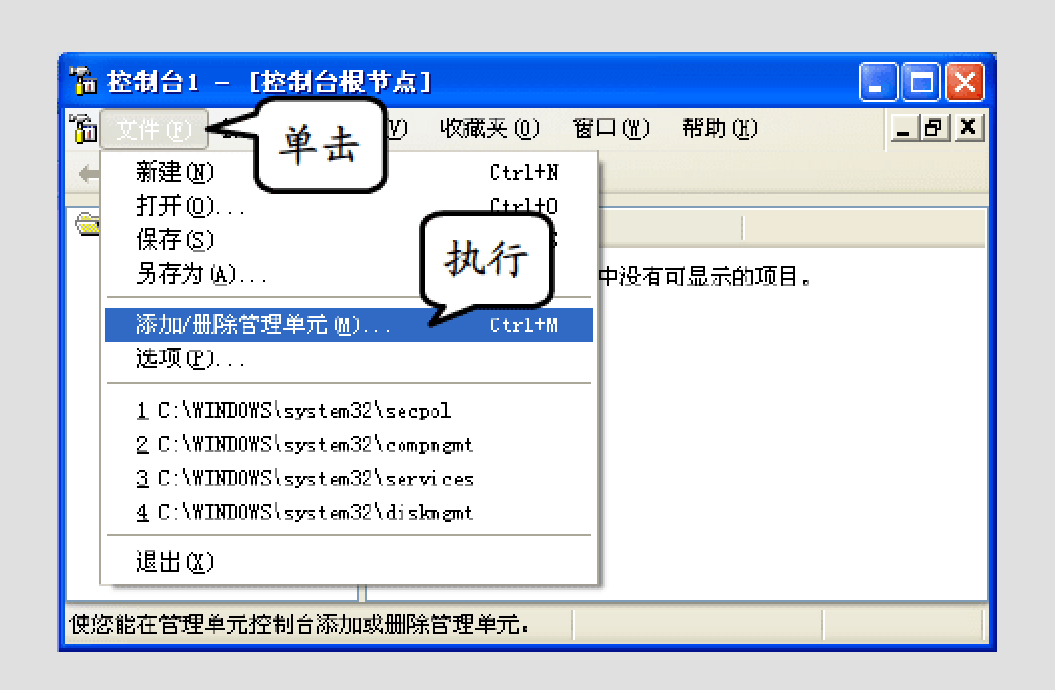


图 5-70 管理控制台主界面



图 5-71 添加独立管理单元

（3）在【添加/删除管理单元】对话框中，单击【确定】按钮，如图 5-72 所示。

（4）在【控制台 1】主界面中，展开【安全模板】节点，并右击 C:\WINDOWS\security\mplates 节点，执行【新加模板】命令，如图 5-73 所示。

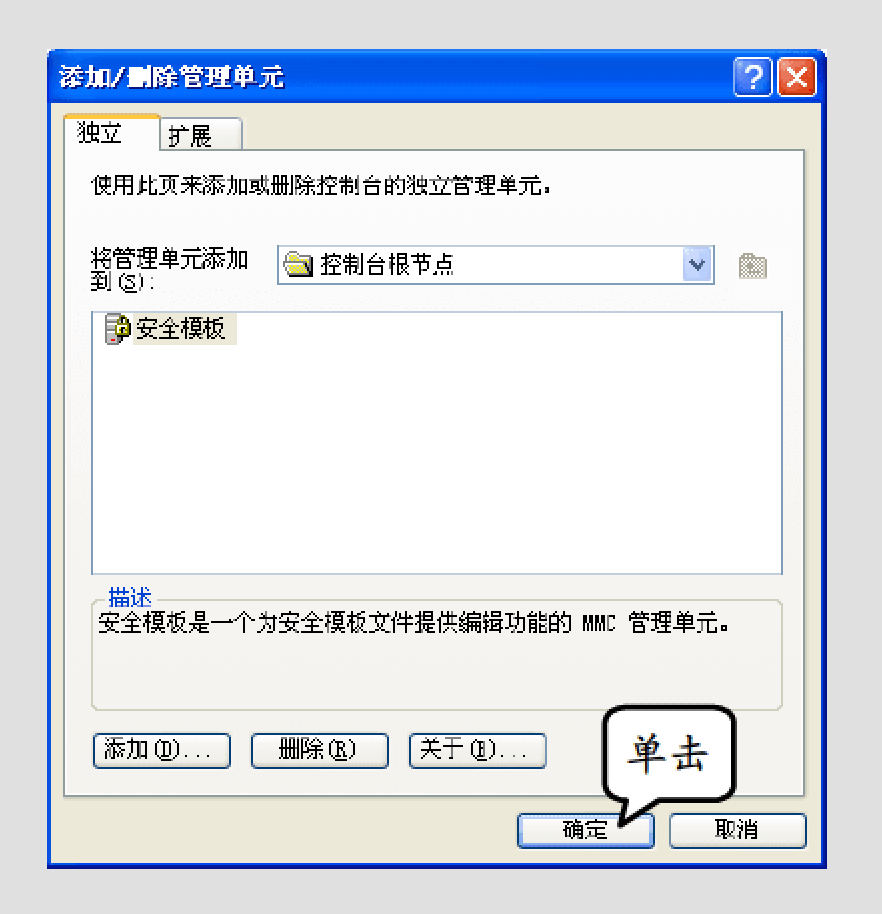


图 5-72 添加安全模板

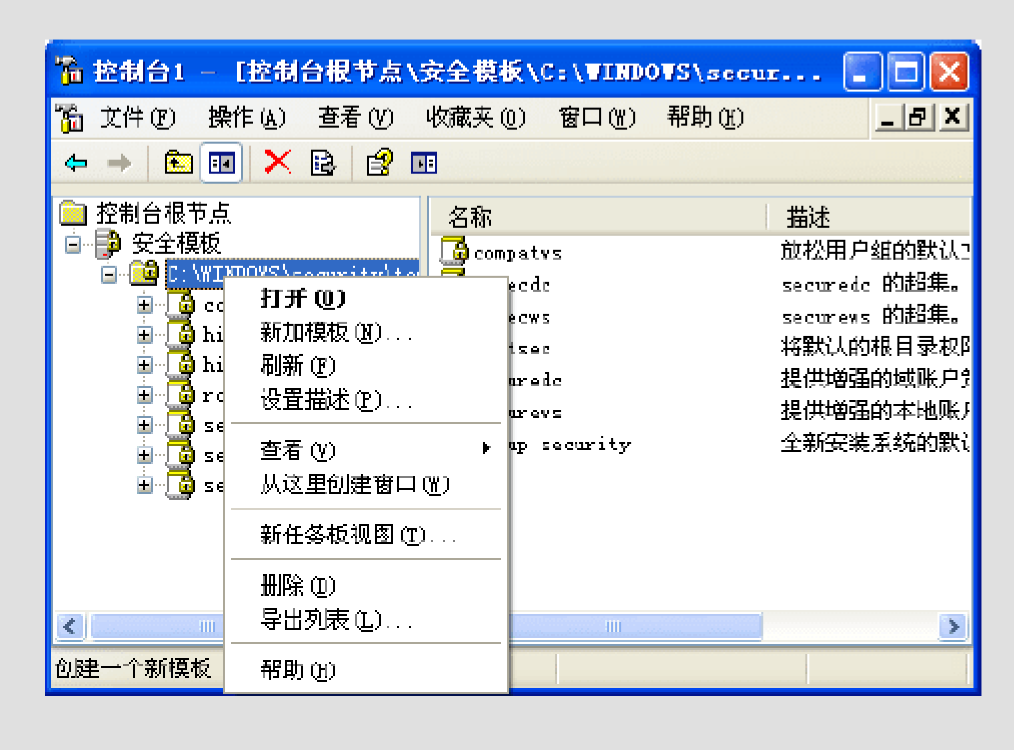


图 5-73 新加安全模板

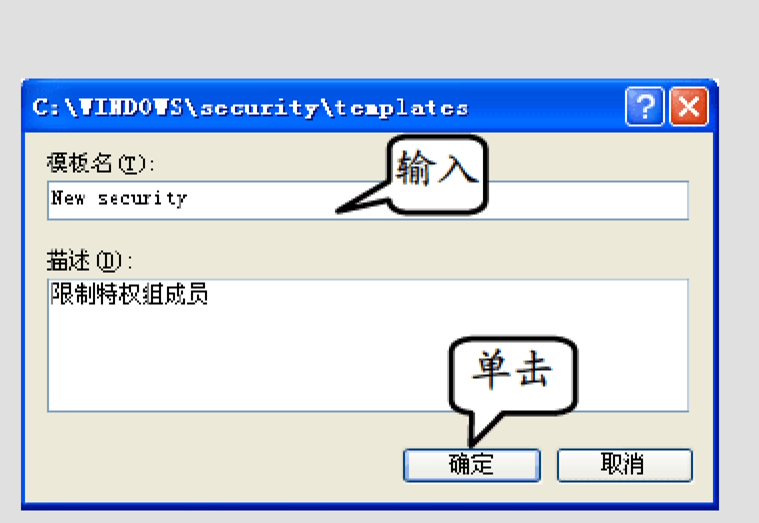


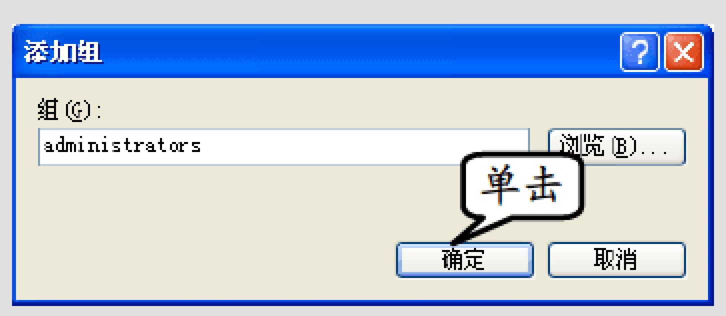
用户可以使用系统默认的安全模板，也可以创建自己需要的新安全模板。

（5）在弹出对话框的【模板名】文本框内输入名称，如“New security”，在【描述】文本框内输入描述内容，如“限制特权组成员”，并单击【确定】按钮，如图 5-74 所示。

（6）在【控制台 1】窗口中，依次展开 New security 和【受限制的组】节点，并在右面窗格任意处右击执行【添加组】命令，在【添加组】对话框中，输入“administrators”（组名），并单击【确定】按钮，如图 5-75 所示。

（7）在弹出的对话框内，单击【添加】按钮，如图 5-76 所示。





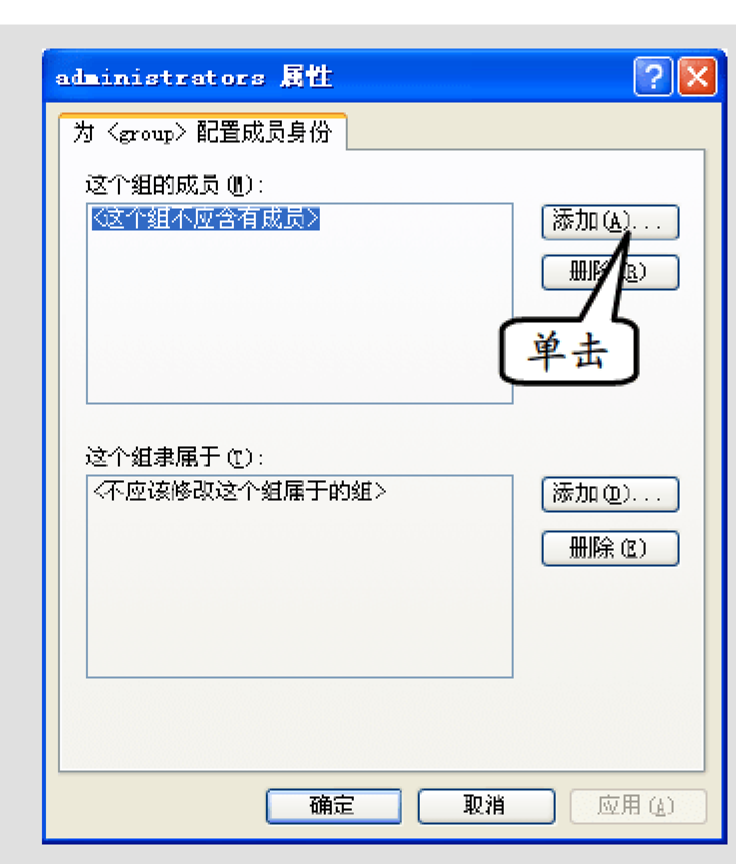
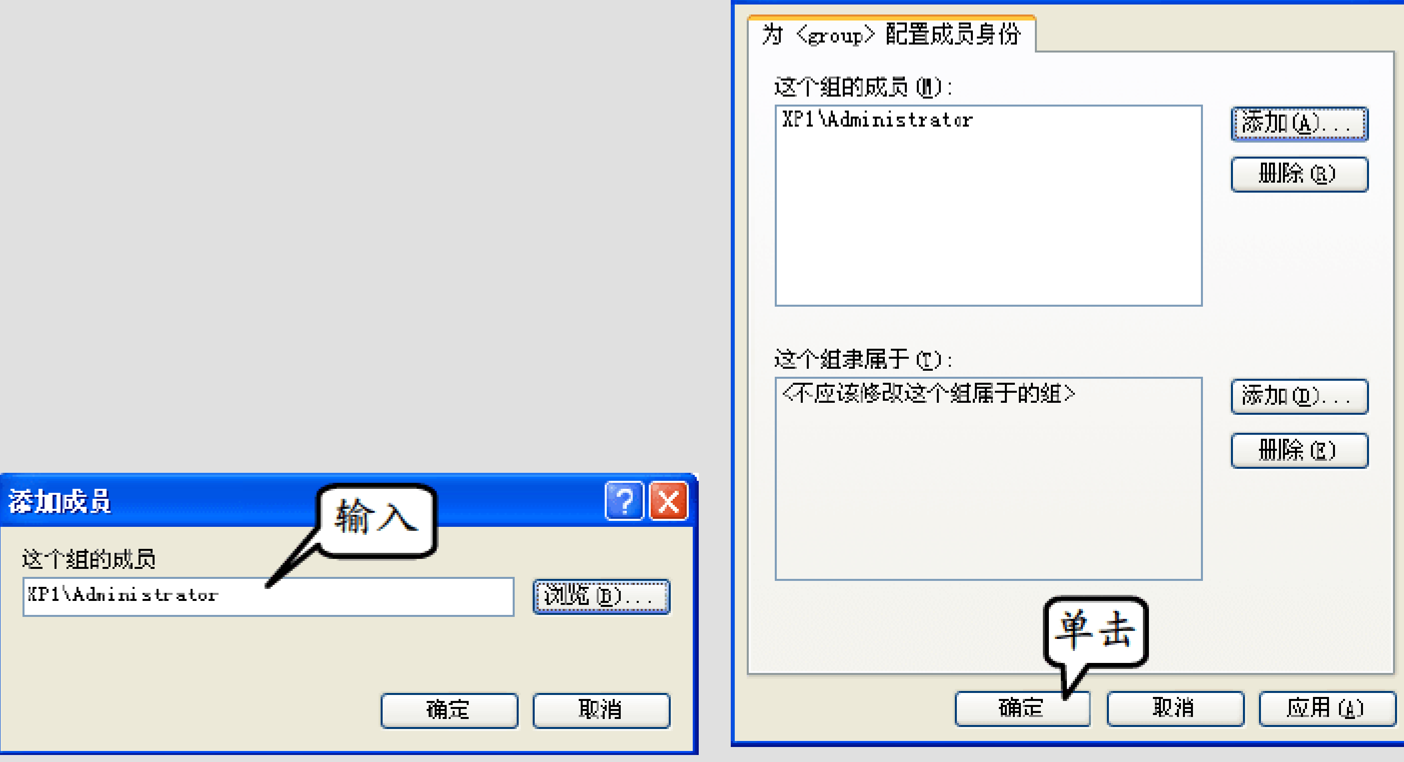


图 5-74　命名模板　　　　图 5-75　添加管理员组　　　　图 5-76　添加管理员的成员

（8）在【添加成员】对话框，输入“XP1\Administrator”（本地管理员），并单击【确定】按钮，如图 5-77 所示。

（9）在【administrators 属性】对话框中，依次单击【应用】和【确定】按钮，如图 5-78 所示。

（10）关闭【控制台 1】主界面，在【保存安全模板】对话框中，单击【是】按钮，如图 5-79 所示。



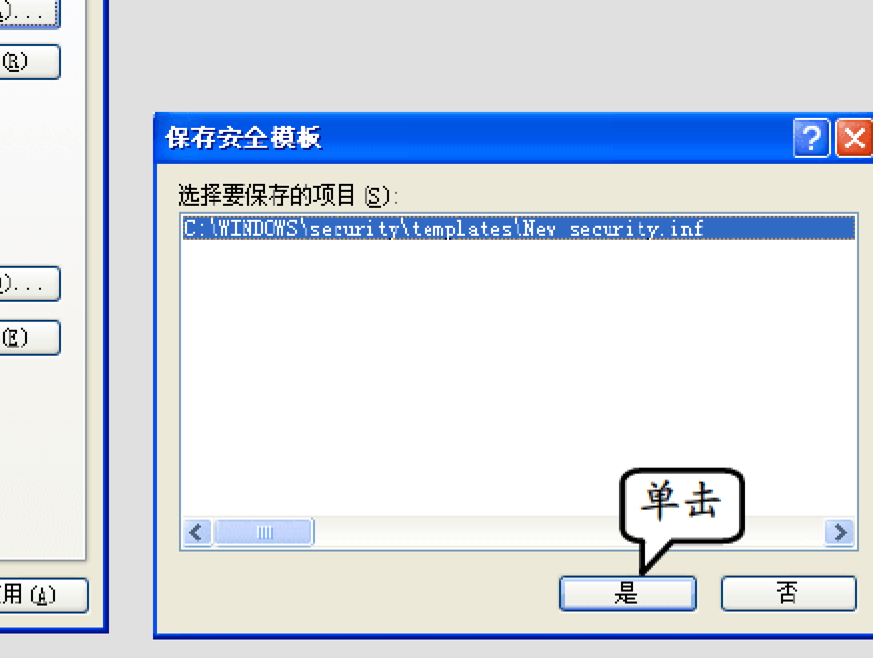


图 5-77　添加成员　　　　图 5-78　应用配置　　　　图 5-79　保存安全模板

（11）在桌面执行【开始】|【运行】命令，在弹出的对话框中输入 cmd 命令，并单击【确定】按钮，在【命令提示符】窗口中，输入 gpupdate /target：computer 命令（刷新计算机策略），如图 5-80 所示。

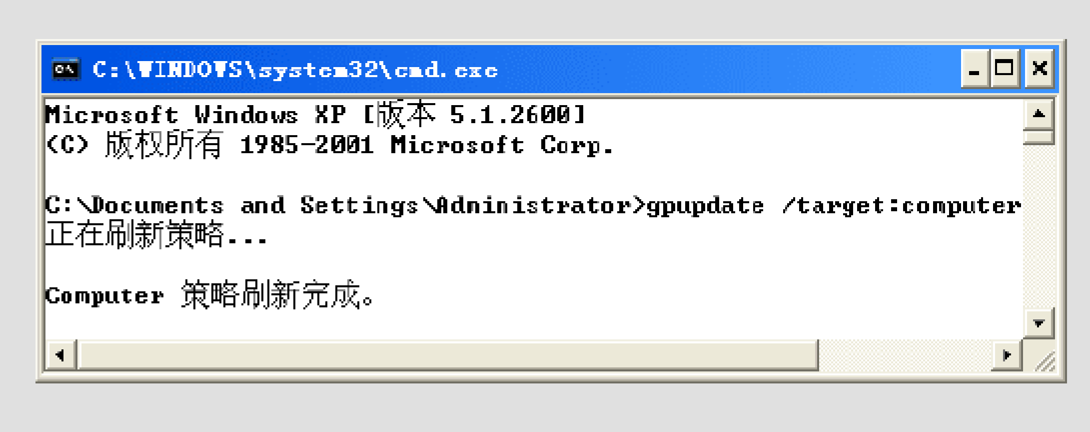


图 5-80　刷新策略

第6章 系统漏洞修补

系统漏洞是指操作系统软件或应用程序软件，在逻辑设计上存在的缺陷或在编写时产生的错误，而这些缺陷或错误有可能被非法用户（如黑客）利用，并将木马程序或病毒等有害程序安装到本地计算机中，从而实现远程控制计算机，窃取用户重要资料和信息，甚至破坏网络系统的目的。

与其他版本的 Windows 操作系统相比，Windows Server 2008 操作系统的安全性已经有了很大的提高，但是几乎每天还会有新的漏洞被发现。目前，及时安装系统更新是应对系统漏洞最有效的方法。本章对系统漏洞的概念、预警、更新等方面的知识进行讲解，使读者充分认识到系统漏洞修补的重要性和必要性。

本章学习要点：

- 了解漏洞的特性、生命周期
- 熟悉漏洞管理流程
- 了解漏洞预警
- 了解 WSUS 及掌握如何配置 WSUS 服务器及客户端的方法
- 熟悉漏洞修补方略

6.1 漏洞概述

客观地讲，系统漏洞是无法避免的，对于 Windows 操作系统而言，新版本操作系统在弥补旧版操作系统漏洞的同时，还会引入一些新的漏洞。这些漏洞，往往会被病毒、木马所利用并入侵计算机系统。应对系统漏洞最好的方法就是制定完善的修补策略，及时修补漏洞。漏洞除了系统（硬件、软件）本身固有的缺陷之外，还包括用户对系统的不正确配置、管理以及制度上的风险，或由其他非技术性因素造成的系统不安全。

6.1.1 漏洞的特性

通常，普通用户都是在产品供应商公布产品漏洞后，才得知漏洞消息的。而从信息安全的角度来讲，是先有漏洞和对漏洞攻击的可能性，才有补丁的出现。漏洞是攻击者所有攻击的目标，而安装补丁是对漏洞的修补过程。漏洞是广泛存在的，在不同的设备、操作系统以及应用系统中都会存在安全漏洞。

漏洞具有自身的特性，通常包括如下 4 个方面。

1. 时间局限性

任何系统漏洞都是在用户不断地使用过程中被发现的，随后系统供应商采取新版本替代旧版本，或是发布补丁程序等方式来弥补漏洞。随着旧漏洞的消失，在新环境下的新漏洞又会随之产生。因此，系统漏洞只是存在于特定的时间和环境下，也就是说，它只能针对目标系统的系统版本、其上运行的软件版本，以及服务运行设置等实际环境。

2. 广泛性

漏洞会影响到大范围的软、硬件设备，包括操作系统本身及其支持的软件平台、网络客户端和服务器软件、网络路由器和安全防火墙等。也就是说，在这些不同的软、硬件设备中，都可能存在不同的系统漏洞问题。例如，不同种类的软、硬件设备之间，同种设备的不同版本之间，以及不同设备构成的不同系统之间，同种系统在不同的设置条件下，都会存在不同的安全漏洞。

3. 隐蔽性

安全漏洞是最常见的系统漏洞类型之一。入侵者借助这些漏洞，可以绕过系统中的许多安全配置，从而达到入侵系统的目的。安全漏洞的出现，是由于对安全协议的具体实现中发生了错误，意外出现的非正常情况。而在实际系统中，都会存在不同程度的潜在错误，因此，在所有的系统中都存在着安全漏洞，无论这些漏洞是否已经被发现，也无论该系统的安全级别如何。在一定程度上，安全漏洞问题是存在于系统本身的理论安全级别上的。也就是说，并不是系统所属的安全级别越高，系统中所存在的漏洞就越少。

4. 被发现性

漏洞是特定环境和时间下的必然产物，只有被发现后，才会被一些人用来入侵系统或弥补系统。在实际使用过程中，用户会发现系统中存在的错误。入侵者会利用其中的某些错误，使其成为威胁系统安全的工具，也就是常说的系统安全漏洞。当系统供应商发现漏洞会尽快发布针对该漏洞的补丁程序，以纠正此错误。这也是系统安全漏洞从被发现到被纠正的一般过程。

6.1.2 漏洞生命周期

由于漏洞造成的安全问题具有一定的时效性，也就是说每一个漏洞都存在一个和产品相类似的生命周期的概念。人们只有对漏洞生命周期的概念进行研究并且分析出它所具有的规律，才能真正解决漏洞危害。

通常生命周期的定义是：漏洞从客观存在到被发现、利用，到大规模危害和逐渐消失，这期间存在一个生命周期，该周期即漏洞生命周期。

以“冲击波（MSBlaster）”蠕虫病毒为例，漏洞生命周期包括如下 5 个基本阶段。

1. 发现漏洞

2003 年 7 月 16 日，微软公司公布了 MS03-026 Microsoft Windows DCOM RPC 接口远程

缓冲区溢出漏洞，该漏洞影响 Windows 2000、Windows XP、Windows Server 2003 系统。

2. 弥补漏洞

2003 年 7 月 16 日，微软公司公布了 MS03-026 补丁用于修补该漏洞。随后，网络上有少数的恶意攻击者利用该漏洞进行入侵。

3. 利用漏洞的病毒大规模爆发

2003 年 8 月 11 日，爆发了利用上述 Windows 漏洞的“冲击波”蠕虫病毒。

4. 病毒出现变种

2003 年 8 月 18 日，出现了一个利用同样原理进行蔓延的“冲击波清除者”病毒，该蠕虫专门清除原来的“冲击波”病毒，但是该病毒同时也消耗大量的 Internet 带宽，从而导致 Internet 性能的明显下降。

在蠕虫爆发后，全球 Windows 用户开始安装 MS03-026 补丁修补该漏洞，网络运营商开始设法阻止蠕虫蔓延，计算机防病毒厂商加入蠕虫特征进行查杀。

5. 逐渐消失

2004 年 1 月，蠕虫传播开始明显得到遏制，微软公司估计全球有 1 000 万台主机受到感染。从整个事件开始到结束，基本可以将漏洞生命周期划分为表 6-1 所示的 5 个阶段。

表 6-1　漏洞的生命周期

阶段	事件	描述
第 1 阶段	系统漏洞被发现，厂商发布漏洞公告	由于软件设计者初期考虑不周等因素导致漏洞客观存在，漏洞研究人员发现漏洞并报告相关厂商，厂商向用户发布安全公告，并提供升级补丁程序
第 2 阶段	借助漏洞传播的病毒开始出现并传播	怀有恶意的攻击者对安全补丁进行逆向工程，编写利用漏洞的攻击程序并发布，由于用户在漏洞管理方面的疏忽，如没有第一时间安装升级补丁程序，从而为蠕虫爆发创造了条件，此阶段漏洞的危害性较小
第 3 阶段	利用漏洞的蠕虫病毒大肆爆发	由于上述的攻击代码和蠕虫程序的实现已经相当成熟，攻击代码很容易被更新为蠕虫代码。蠕虫在互联网上或者局域网中，利用系统漏洞大规模传播，导致网络堵塞或者瘫痪
第 4 阶段	系统漏洞被修复，但仍有发作	由于安装系统补丁，蠕虫丧失感染目标，已经感染的主机逐步清除使蠕虫源减少。没有安装补丁的主机数量减少，对网络的影响不大
第 5 阶段	漏洞影响逐渐消失	一段时间后，由于系统升级或者完成系统补丁的安装工作，或者使用新的软件版本，漏洞造成的影响逐步消失

6.1.3　漏洞扫描概述

漏洞扫描是网络安全防御中的一项重要技术，其原理是采用模拟攻击的形式对目标可能

存在的已知安全漏洞进行逐项检查。检查的目标可以是工作站、服务器、交换机和数据库等，在扫描结束后，可以向管理员提供一份周密可靠的安全性评估报告，从而为提高网络安全整体水平提供重要依据。

在网络安全体系的建设中，单机安全扫描是一种花费低、效果好、见效快、与网络运行相对独立、安装运行简单的工具，可以大规模减少网络管理员的手工操作，有利于保持全网安全的统一和稳定。

目前，市场上存在很多漏洞扫描工具，根据不同的技术（基于网络的、基于主机的、基于代理的、Client/Server）、不同的特征、不同的报告方式，以及不同的监听模式，漏洞扫描工具可以分成多种类型。而不同的产品之间，漏洞检测的准确性差别较大，这也决定了在生成报告有效性上的区别。选择正确的漏洞扫描工具，对于提高系统的安全性非常重要。

1. 漏洞扫描的必要性

一般情况下，在网络边界处都会部署硬件或软件防火墙。防火墙作为不同网络或网络安全区域之间信息的唯一出口，能根据企业的安全政策控制（允许、拒绝、检测）出入网络的信息流，且本身具有较强的抗攻击能力。虽然防火墙是提供信息安全服务、实现网络和信息安全的基础设施，但是，它本身也存在一定的局限性。

一般局域网都具有“外紧内松”的特点，一道严密防守的防火墙的内部网络也有可能防范松懈。因此，进行漏洞扫描很有必要。

2. 扫描工具的技术性能

采用漏洞扫描工具是保护系统安全的重要一步。当决定进行漏洞扫描之后，接下来就是如何选择满足企业需要、合适的漏洞扫描软件或者工具。

通常，在选择漏洞扫描工具时，应当注意以下几个方面的问题。

- 漏洞库中的漏洞数量。
- 扫描工具的易用性。
- 是否可以产生漏洞报告，包括内容是否全面、是否可配置、是否可定制、报告的格式和输出方式等。
- 对于漏洞修复行为的分析和建议。是否只报告存在哪些问题、是否会告知应该如何修补这些漏洞。
- 安全性。由于有些扫描工具不仅仅只是发现漏洞，而且还进一步利用这些漏洞，扫描工具自身是否会带来安全风险。
- 工具或软件的性能及价格。

6.1.4　网管心得——漏洞管理流程

目前，绝大部分的网络攻击都是借助目标网络的漏洞实现的。网络中常规的安全设备，如防火墙、入侵检测系统（IDS）、统一威胁管理（UTM）等，很难阻止这种恶意攻击。要从根本上解决利用漏洞进行攻击的问题，就需要对漏洞产生的原因、漏洞的生命周期进行研究，同时还要配合人为的管理模式，建立行之有效的管理机制，并通过漏洞管理类产品来辅助管

理员执行漏洞管理。

1. 安全策略

安全策略是确保服务器、网络设备、客户端计算机以及网络安全设备能够正常工作的安全配置。目前，大部分网络设备都能够提供丰富的安全功能，并且部分功能已经默认启用，用户可以根据实际需要，制定更加详细的安全策略。

2. 漏洞预警

漏洞预警是指产品供应商在发现漏洞后，第一时间告知用户所采取的工作。漏洞供应商通常会提供相应的补丁程序，如果没有相应的补丁程序，应给出临时解决方案。

3. 漏洞检测

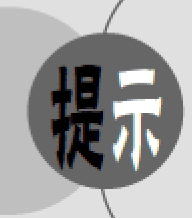
在进行漏洞检测工作之前需要对网络进行发现和跟踪，以便快速、准确地确定产生漏洞的计算机或网络设备。作为网络管理员，必须周期性地对网络中的网络资产进行检测，要求漏洞管理工具在保证一定效率的前提下，具有较高的准确性。



在进行漏洞检测时，并不是检测到的漏洞越多越好，更重要的是要对检测出漏洞的有效性进行验证和分析。

4. 漏洞统计分析

当漏洞检测工作完成后，需要网络管理员通过具体的报告和数据对资产的风险进行评估和分析，清晰明了地显示出漏洞分布状况、详细描述以及制定相应的解决方案。



网络管理员应当对网络中存在的资产风险进行分类，以便于能够对后续的漏洞修补工作进行优先级区分。这一过程也可以通过购买专业的漏洞管理设备或者安全服务来完成。

5. 漏洞修补

通过统计分析的结果制定切实可行的漏洞修补方案，并以合理的方式通知用户，例如，通过自动更新服务器来提供最新的漏洞修补程序，用户可以按需进行下载安装，也可以由服务器自动分发完成。

在漏洞修补阶段要注意补丁程序来源的合法性，以及补丁的安全性。通常，必须对补丁程序进行小范围内的安全性和兼容性测试，在确保补丁程序不会影响到业务系统的正常运行之后，方可大规模分发及安装。

6. 漏洞审计、跟踪

在网络中，必须部署完善的漏洞审核机制，即对于新接入或启用的计算机或网络设备，应该进行补丁状态检测，如果不能满足安全要求，那么就要拒绝其继续访问网络，或通过其

他措施使其可以获得所需的安全补丁。这个过程可以通过操作系统厂商、第三方的补丁管理软件或者专业的安全服务来完成。

7. 其他问题

一个完善的漏洞管理机制应该能够有效地保证人为的管理疏漏不会被攻击者利用，这对于大多数利用漏洞进行的攻击会十分有效。

网络管理人员在制定漏洞管理流程的时候，需要根据实际情况进行细化或者裁减，以确保漏洞管理的高效、灵活和实用。另外，漏洞管理流程应该注意以下问题。

- 工作流程标准化。
- 尽量实用专业的、自动化的漏洞管理工具，尽量避免人为操作。
- 尽量不要中断企业的业务流程，保证业务能够正常运行。
- 漏洞修补尽量安排在晚上或者业务不繁忙的时间段进行。
- 在测试环境中模拟测试通过，在确保不影响当前业务状态的情况下，实施漏洞修补工作流程。
- 针对不同的操作系统要准备不同版本的补丁程序。

6.2　操作实例一

6.2.1　操作实例——MBSA 工具

Microsoft Baseline Security Analyzer（MBSA）工具允许用户扫描一台或多台基于 Windows 操作系统的计算机，并检查操作系统和已安装的其他组件，以发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。

1. 实例目的

- 扫描系统漏洞和安全风险。
- 扫描 Windows 组件及应用程序。
- 实现系统的安全更新与配置。

2. 实例步骤

（1）在桌面双击 Microsoft Baseline Security Analyzer 6.2 应用程序图标，如图 6-1 所示。

（2）在软件主界面中，单击【扫描一个电脑】按钮，如图 6-2 所示。

（3）在【选择要扫描的计算机】对话框中，禁用【检查 IIS 漏洞】和【检查 SQL 漏洞】复选框，并单击【开始扫描】按钮，如图 6-3 所示。



如果计算机安装了 Web 服务和 SQL Server 软件，则启用【检查 IIS 漏洞】和【检查 SQL 漏洞】复选框。



图 6-1　执行应用程序

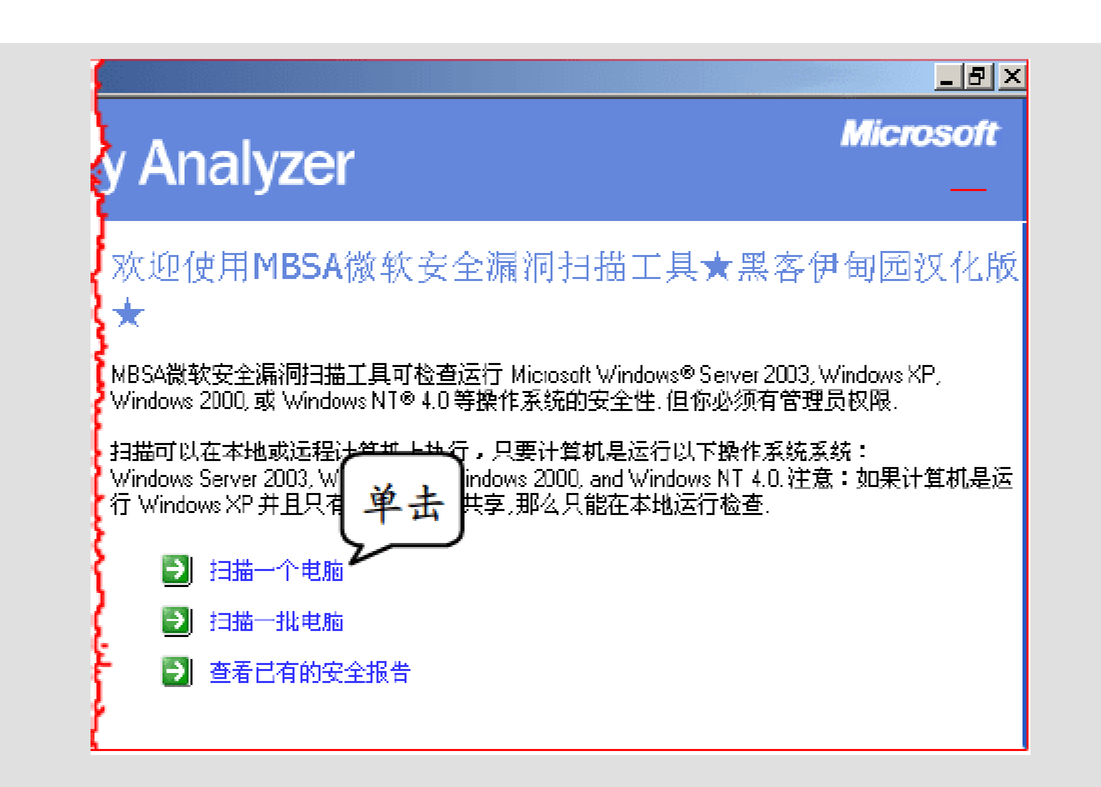


图 6-2　主界面

（4）在【查看安全性报告】窗口中，可查看到安全性报告的详细信息，如图 6-4 所示。

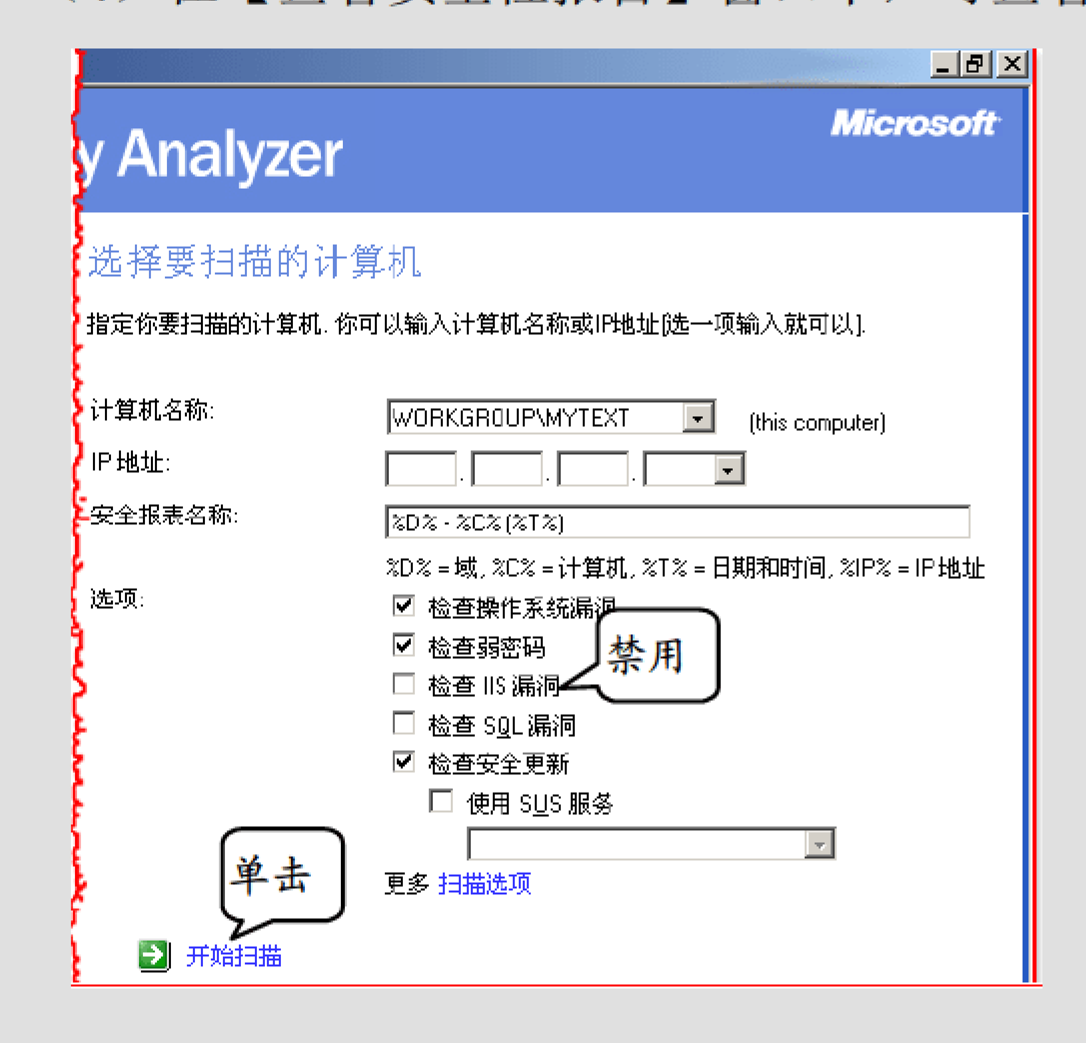


图 6-3　选择要扫描的计算机窗口



图 6-4　查看报告内容

6.2.2　操作实例——奇虎 360 安全卫士

360 安全卫士具有强大的模块扫描能力，能够发现系统深层隐藏漏洞，并且拥有完善准确的系统补丁数据库，保证系统安全可靠地运行。

1. 实例目的

- ❑ 发现系统及应用程序漏洞。
- ❑ 修复漏洞。
- ❑ 更新 Windows 系统补丁。

2. 实例步骤

（1）在桌面上双击【360 安全卫士】图标，如图 6-5 所示。

（2）在【360 安全卫士 V6.1.5】的主界面窗口中，选择【修复漏洞】选项卡，如图 6-6 所示。

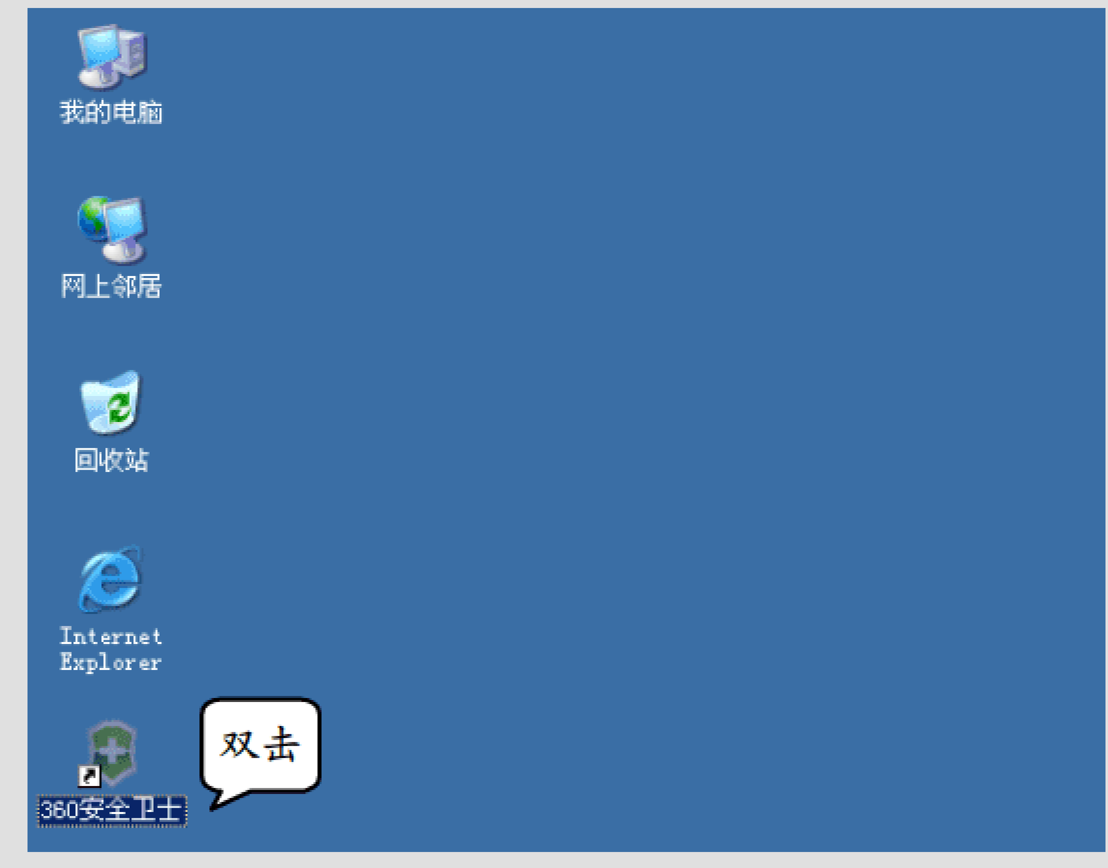


图 6-5　执行应用程序



图 6-6　主界面

（3）当该软件检测系统漏洞结束后，在【修复漏洞】选项卡内，单击【修复】按钮，如图 6-7 所示。

（4）在【修复漏洞】选项卡内，可查看到修复结果，并单击【立即重启】按钮，如图 6-8 所示。





图 6-7　【修复漏洞】选项卡

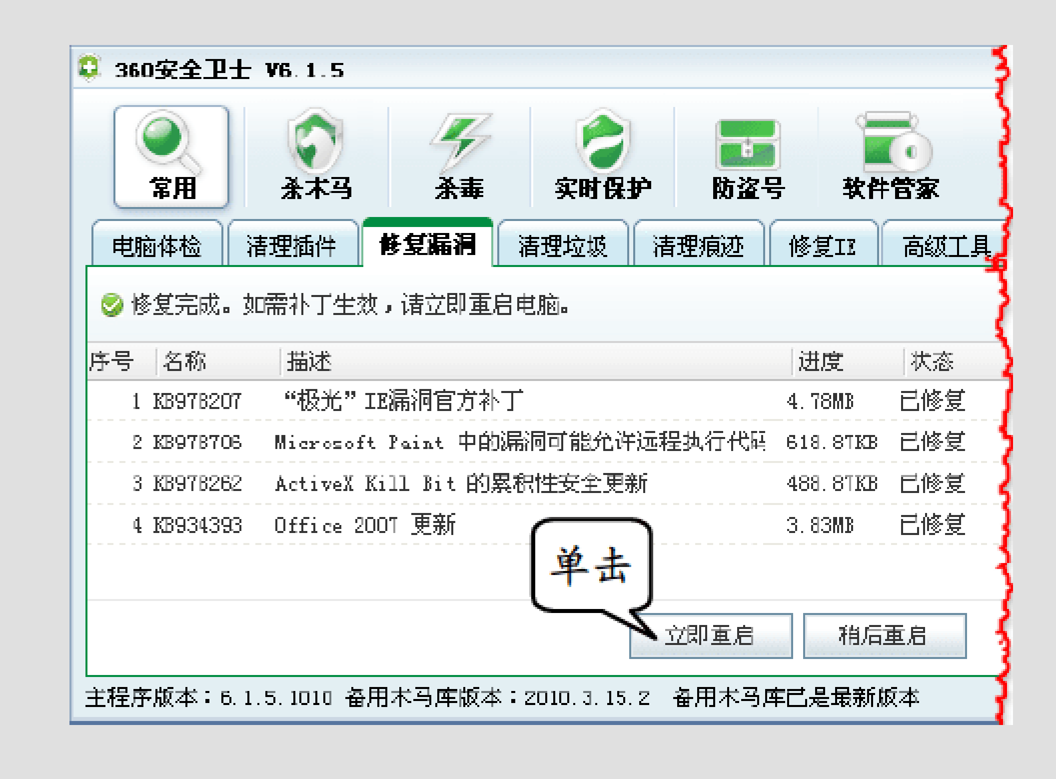


图 6-8　查看修复结果

6.2.3　操作实例——瑞星漏洞扫描工具

瑞星卡卡上网助手能够自动修复操作系统漏洞、第三方软件漏洞和相关安全设置，使计算机被病毒破坏的系统设置恢复正常。

1. 实例目的

- ❑ 快速扫描系统漏洞和安全缺陷。
- ❑ 扫描第三方软件更新。
- ❑ 强力修复系统及应用软件漏洞。

2. 实例步骤

（1）在桌面上双击【瑞星卡卡上网安全助手】图标，如图 6-9 所示。

（2）在【瑞星卡卡上网安全助手】主界面窗口【常用】选项卡内，单击【漏洞扫描与修复】图标，如图 6-10 所示。



图 6-9　执行应用程序



图 6-10　【瑞星卡卡上网助手】主界面窗口

（3）在【系统漏洞】选项卡内启用需要修复选项的复选框，并单击【修复所选项】按钮，如图 6-11 所示。

（4）在【系统漏洞】选项卡内可查看到修复结果，如图 6-12 所示。



图 6-11　系统漏洞选项卡



图 6-12　修复结果窗口

6.3　漏洞预警

漏洞预警工作通常由产品供应商完成，也就是说确保在漏洞发现后，能够第一时间告知用户，如果没有相应的补丁程序，还应给出临时的解决方案等。这就要求漏洞管理产品的厂商应该有基础的漏洞研究、跟踪以及提供临时解决方案的能力。

6.3.1　中文速递邮件服务

中文速递邮件是微软中文帮助以及支持网站为更好地服务于中国客户而提供的一种免费服务，该邮件一月一刊，自动发送到用户指定邮箱，帮助用户及时了解最新微软软件的热点问题、帮助指南以及最新下载。

通过 TechNet 中文速递邮件服务，企业网络管理人员能够了解到当前各项技术信息、技术资源、故障与疑难诊断、安全性信息、培训信息等，例如，免费的 TechNet 技术讲座、网络广播、虚拟实验室、技术指引视频等。

另外，中文速递邮件中包括了微软最新安全公告，有关 Microsoft 产品和所有有价值的技术信息，以及 Microsoft 提供的最新服务包和知识库文章。该邮件也会将当前重大病毒信息在第一时间报道给客户，并提醒客户对系统做安全防护。

用户需要注册订阅 TechNet 中文速递邮件，在订阅后才可以收到安全公告、TechNet 活动信息、技术资源库、热门知识库文章、最新服务包、TechNet 网络广播、下载及测试版软件等重要资讯和技术内容。用户在注册成功后，或者是已经收到 TechNet 中文速递邮件，还可以根据个人需求及技术爱好，订制自己的 TechNet 中文速递邮件，获取对自己最重要的资讯，图 6-13 所示为 2010 年第 5 期的 TechNet 中文速递邮件。



图 6-13　TechNet 中文速递邮件

6.3.2　安全公告网络广播

目前，企业及其他各行各业对于网络的依赖性越来越强，而网络中存在的各种安全性风险，已经严重威胁了企业内部数据的安全。那么，除了硬件安全性的构建外，作为网络中经常变化的，汇聚大部分企业信息的主机及相关节点的安全性，就成为每个管理员必须面对的问题。毫无疑问，无论哪种操作系统都不能够保证完全没有漏洞，但问题的关键是如何及时发现漏洞并对其进行修复。

微软安全响应中心（Microsoft Security Response Center，MSRC）就是微软内部一个这样

的机构，由它自主研发并接受来自第三方安全公司及客户的反馈，在确认问题后，于美国时间每个月的第 2 个星期二发布相应的补丁及应对方案。相应地，微软中国随后也会在北京时间每个月的第 2 个星期三执行同步发布，并在星期五发布中国区安全公告网络广播（Webcast）。

安全公告网络广播通常由微软讲师来指导用户理解微软最新的安全公告，并讲解如何针对该安全性公告，在企业内部进行安全性修复。同时，也会提到安全指导建议，这将会指导用户面对企业环境，如果不能及时安装补丁，如何采取一个紧急应对措施，以避免企业数据遭到破坏，为随后执行的安全性修复赢得时间。

安全公告网络广播（Webcast）也会覆盖当月的微软产品更新，工具更新及相关信息。企业管理员都会在自己的管理经历中，意识到一个问题，那就是微软发布的安全性修复往往同企业内部复杂的应用环境存在差距，那么如何在保障生产环境正常运作的前提下，应用这些安全性修复，就需要企业管理员对于安全性修复有足够的认识，并结合实际环境予以测试。这就需要关注安全公告网络广播，图 6-14 所示为所有 Microsoft 安全公告摘要和网络广播。

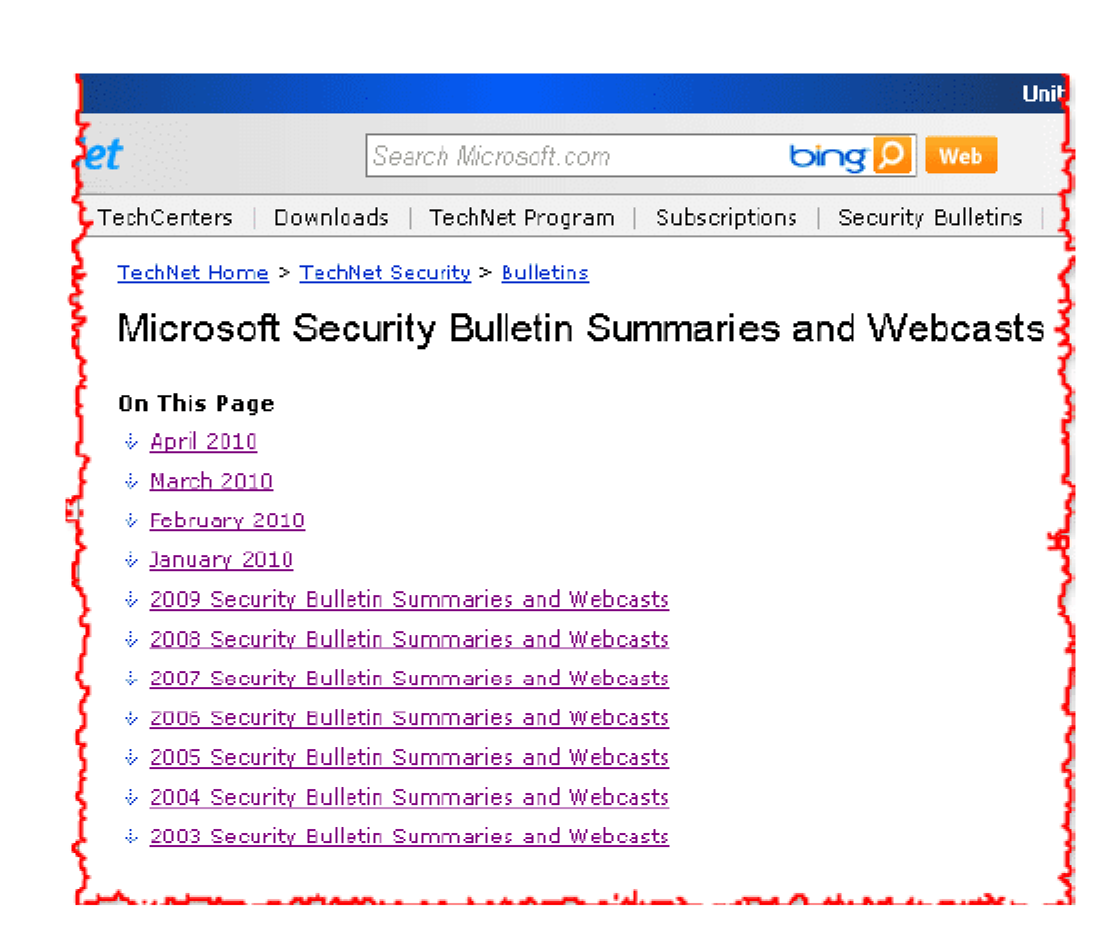


图 6-14　Microsoft 安全公告摘要和网络广播

安全公告网络广播的主要目的是给广大用户提供一个可以向微软安全专家咨询有关微软安全公告和补丁管理相关信息的机会，同时微软安全专家也会在广播中为用户解答在日常工作中碰到的相关问题。

通常用户需要在微软官方网站在线注册申请收听当月的安全公告网络广播，这些安全公告网络广播将以点播的方式为用户提供。在此日期之后，该网络广播将按需为用户提供。

6.4　漏洞更新

系统不完善就会出现漏洞，在网络中更是如此，漏洞验证威胁计算机及整个网络的安全，因此，在发现漏洞以后及时安装由计算机软件、硬件供应商提供的补丁程序对系统安全是很重要的。

6.4.1　WSUS 概述

WSUS（Windows Software Update Service）是微软公司推出的免费网络化补丁分发方案，可以从微软网站中下载获得并安装。WSUS 支持微软公司全部产品更新，使网络管理员能够将最新的 Microsoft 产品更新部署到客户端计算机上。

通常，家庭或中小型用户都是直接从 Microsoft Update 服务器下载所需更新程序进行安装。但是，对于大型网络，如果仍然采用这种方式，那么每天仅此一项网络流量就可能占去一大部分。而通过 WSUS 这个内部网络中的 Windows 升级服务，就可以让所有的 Windows 更新都

集中下载到内部网的 WSUS 服务器中，使网络中的客户机通过 WSUS 服务器得到更新。这不仅节省了网络资源，避免了网络流量的浪费，而且提高了内部网络中计算机的更新效率，图 6-15 所示为 WSUS 体系结构示意图。

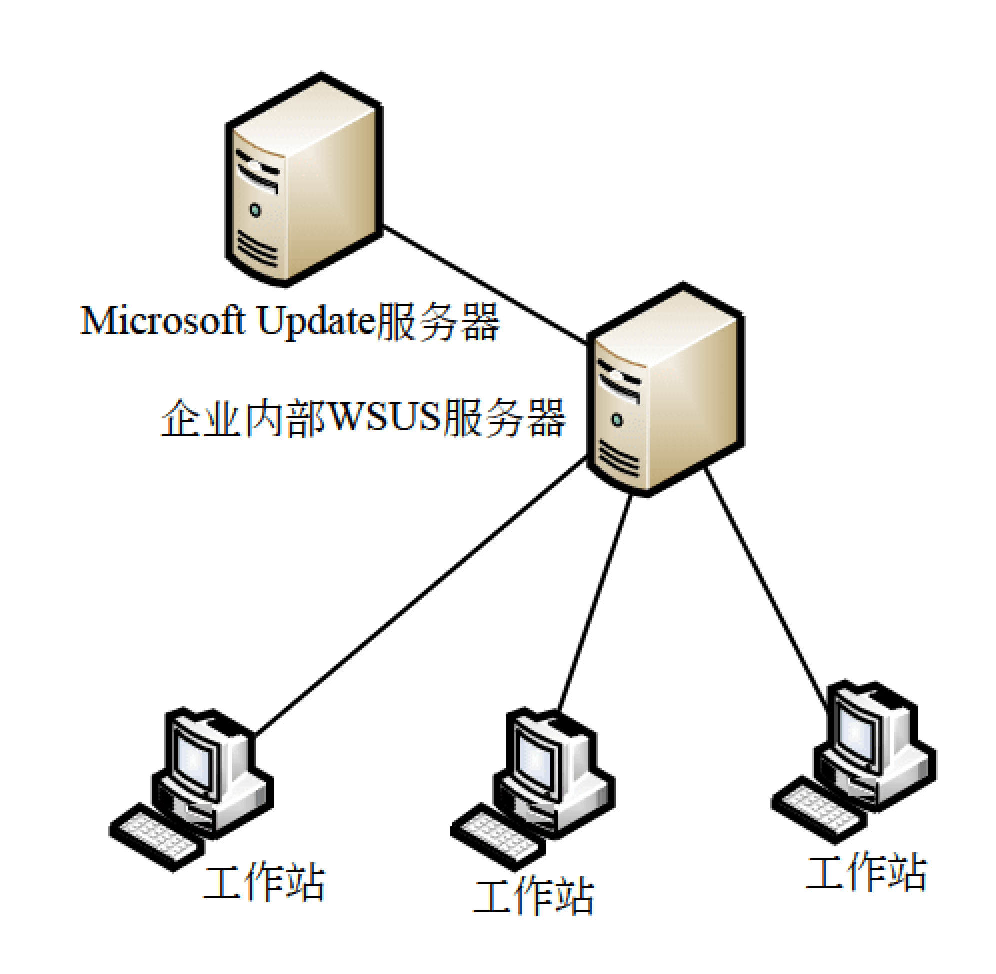


图 6-15 WSUS 体系结构

如果企业网络规模比较大，还可以采用多级 WSUS 结构，如图 6-16 所示。其中，“上游”WSUS 升级服务器负责从 Microsoft Update 站点下载升级补丁并管理“下游”的 WSUS 升级服务器，而“下游”的 WSUS 升级服务器从“上游”的 WSUS 升级服务器获得补丁，并为企业网络中的工作站提供升级补丁。所有的工作站被划分到不同的“下游”WSUS 升级服务器中并且从其设置的“下游”WSUS 升级服务器处获得补丁。

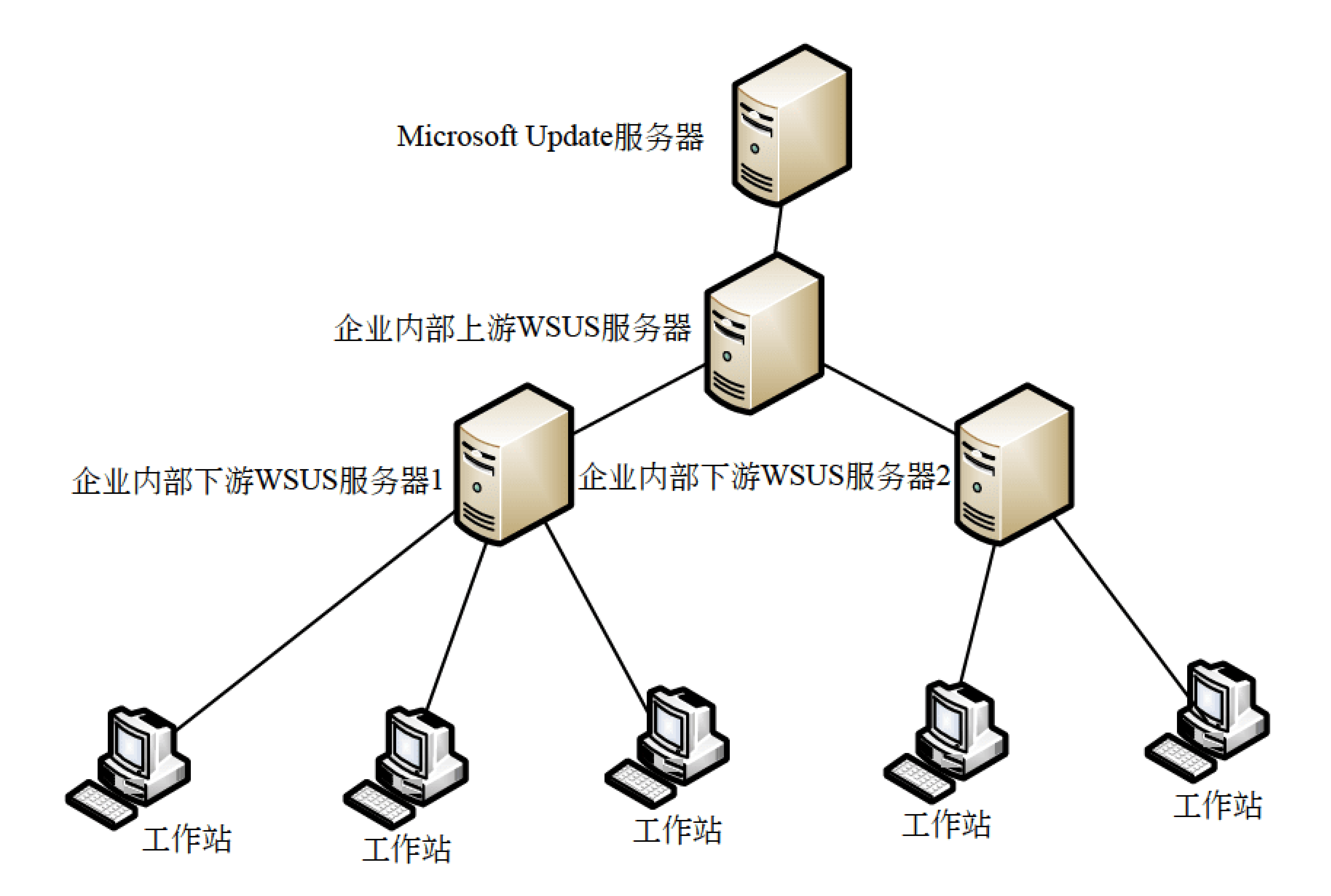


图 6-16 多级 WSUS 体系结构

WSUS 是一款服务器/客户端模式的软件，应用之前应先正确配置服务器端。安装 WSUS 服务器时，必须使用具有本地管理员权限的用户账户登录系统。

1. 软件需求

在 Windows Server 2008 中，可安装的 WSUS 3.0 SP2 程序，对操作系统版本、操作系统上运行的服务、IIS、数据库、磁盘分区格式以及硬盘可用空间都有一定的要求。这包括如下几个方面。

- ❑ WSUS 服务器系统平台可以是 Windows Server 2003 SP1/SP2、Windows Server 2003 R2、Windows Server 2008 SP1 或 Windows Server 2008 R2。

- 目标服务器不能安装“终端服务”，如果确认需要使用“终端服务”对计算机进行管理，则可以在安装 WSUS 之前临时将其删除，或在安装 WSUS 以后再安装“终端服务”即可。
- 需要 IIS 6.0/7.0 的支持。
- WSUS 根服务器必须可以连接到 Internet，如果使用代理服务器连接 Internet，则代理服务器必须支持 HTTP 或者 HTTPS 方式。
- 安装 WSUS 时，需要退出正在运行的反病毒软件和一切防火墙软件。
- 如果在网络中配置需要协同工作的多台 WSUS 服务器，那么需要安装专用的 SQL Server 2005/2008 数据库，安装程序默认安装的数据库（WMSDE）只能用于独立的 WSUS 服务器。
- 如果安装 WSUS 服务器操作系统为 Windows Server 2008，则满足系统需求即可，如果是 Windows Server 2003，那么除满足系统运行需求外，还必须确保内存不低于 512MB。

2. 硬件需求

WSUS 3.0 SP2 在功能上虽然有了明显提升，但在硬件需求方面变化不大。在企业网络中，如果客户端计算机数量不大于 500 台，WSUS 服务器的主要硬件配置信息如下所示。

- 至少为 1GB 内存。
- 处理器至少为 1GHZ 或更高。
- 磁盘空间根据所选数据库的不同而有所区别，建议保留 30GB 的自由空间用于存储下载数据和数据库信息。
- 确保 WSUS 服务器到 Internet 以及和客户端之间的网络连接正常。

3. 准备工作

在即将安装 WSUS 的计算机中，安装 Windows Server 2008 操作系统以及各种驱动程序，配置网卡的 IP 地址、子网掩码、网关及 DNS 参数，使其可以连接到 Internet，如果通过代理服务器连接 Internet，应指定正确的代理服务器信息和有效的身份凭证。

另外，在安装 WSUS 之前，还应该做好如下准备工作。

- 安装 IIS 服务。
- 后台智能传输服务（BITS）2.0。
- Report Viewer（可选组件，但建议安装）。



在安装 IIS 过程中，应确保启用【应用程序开发】列表中的 ASP.NET 复选框，否则将无法完成 WSUS 的安装。

6.4.2 配置 WSUS

在 Windows Server 2008 中，当用户从微软网站下载 WSUS 3.0 SP2 安装程序安装结束时，

还需要对 WSUS 服务器进行配置，才可以使 WSUS 服务器开始工作，这包括设置服务器接入 Internet 方式、获取更新方式、支持产品分类、同步方式及时间等内容。

当安装结束后，在弹出的【在您开始之前】对话框中，直接单击【下一步】按钮，接着，在【加入 Microsoft Update 改善计划】对话框中，启用【是的，我希望加入 Microsoft Update 改善计划】复选框，并单击【下一步】按钮，如图 6-17 所示。

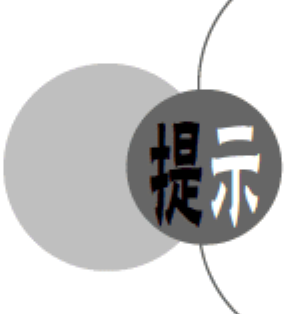
在【选择“上游服务器”】对话框中，系统默认选中【从 Microsoft Update 进行同步】单选按钮，即直接从微软服务器获取更新程序。如果网络中已经存在“上游 WSUS 服务器”则可以选中【从其他 Windows Server Update Services 服务器进行同步】单选按钮，并在【服务器名】文本框中，输入上游 WSUS 服务器的 IP 地址或计算机名，在【端口号】文本框中，输入上游 WSUS 服务器的端口号即可，如图 6-18 所示。



图 6-17 加入 Microsoft Update 改善计划



图 6-18 选择上游服务器



选择本地网络的上游 WSUS 服务器时，如果使用的上游服务器使用了 SSL 通信方式，则在此处应当启用【在同步更新信息时使用 SSL】复选框。但是，部署 SSL 会增加 WSUS 服务器大约 10%左右的工作负荷，并且这种传输加密机制仅能用于 WSUS 数据通信，而并非是所有需要传输的更新文件。

在【指定代理服务器】对话框中，如果使用代理服务器与 Internet 连接，以便于 Microsoft Update 进行同步更新，则可启用【在同步时使用代理服务器】复选框，并在【用户名】、【域】和【密码】文本框中输入相应的用户凭证；反之，则直接单击【下一步】按钮，如图 6-19 所示。

在【连接到上游服务器】对话框中，单击【开始连接】按钮，如图 6-20 所示，以便在服务器上配置 Windows Server Update Services，当连接完成后，直接单击【下一步】按钮。

在【选择“语言”】对话框中，选择此服务器将下载的更新语言，此时，可以选中 Download updates only in these languages 单选按钮，并启用该列表中相应的复选框即可，如图 6-21 所示。

在【选择“产品”】对话框中，可以指定需要更新的产品，如启用【所有产品】复选框，则 Microsoft 公司的所有产品的更新都将被下载，单击【下一步】按钮，如图 6-22 所示。

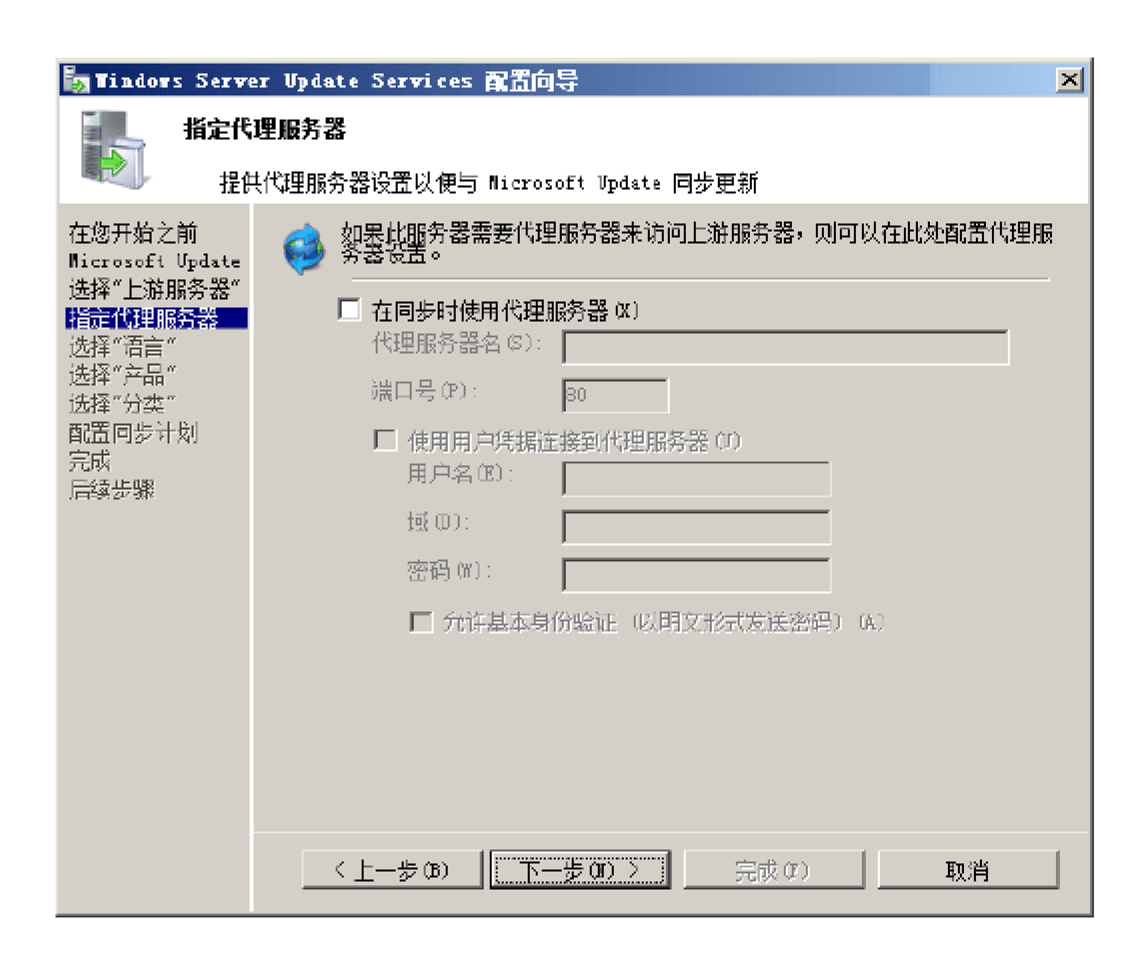


图 6-19　指定代理服务器

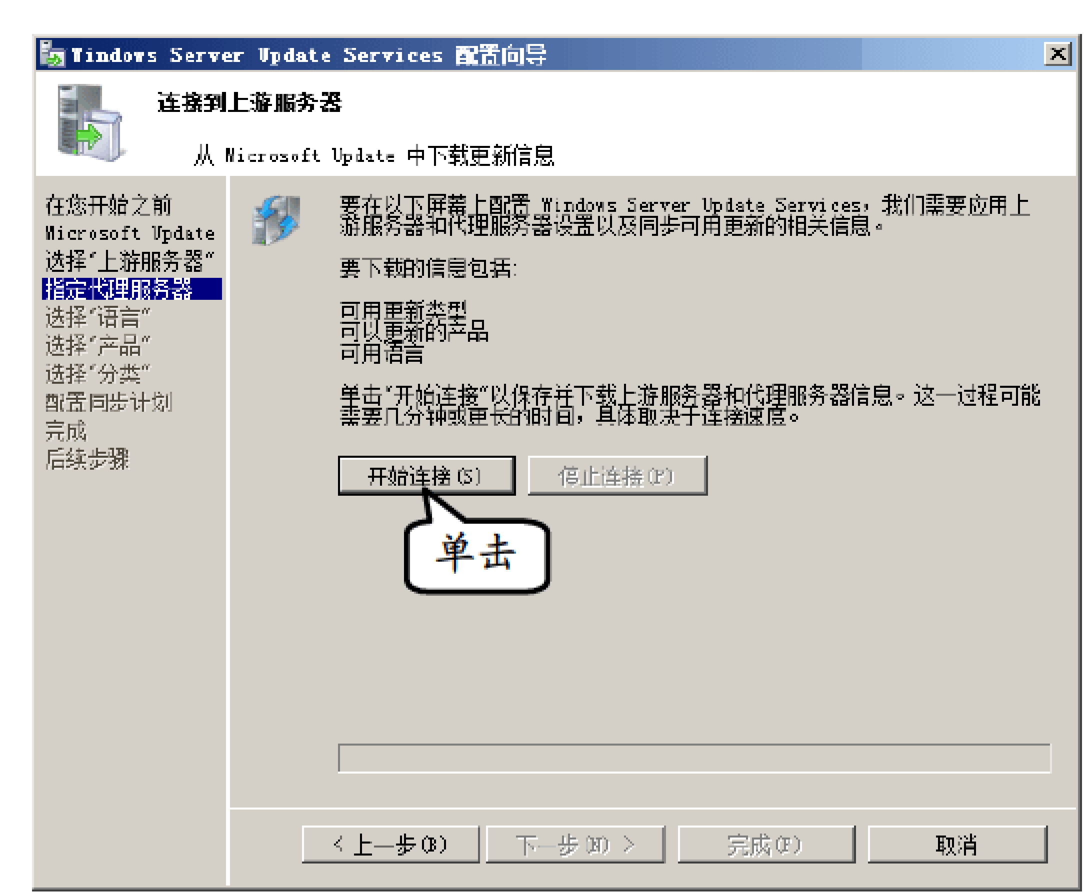


图 6-20　连接上游服务器

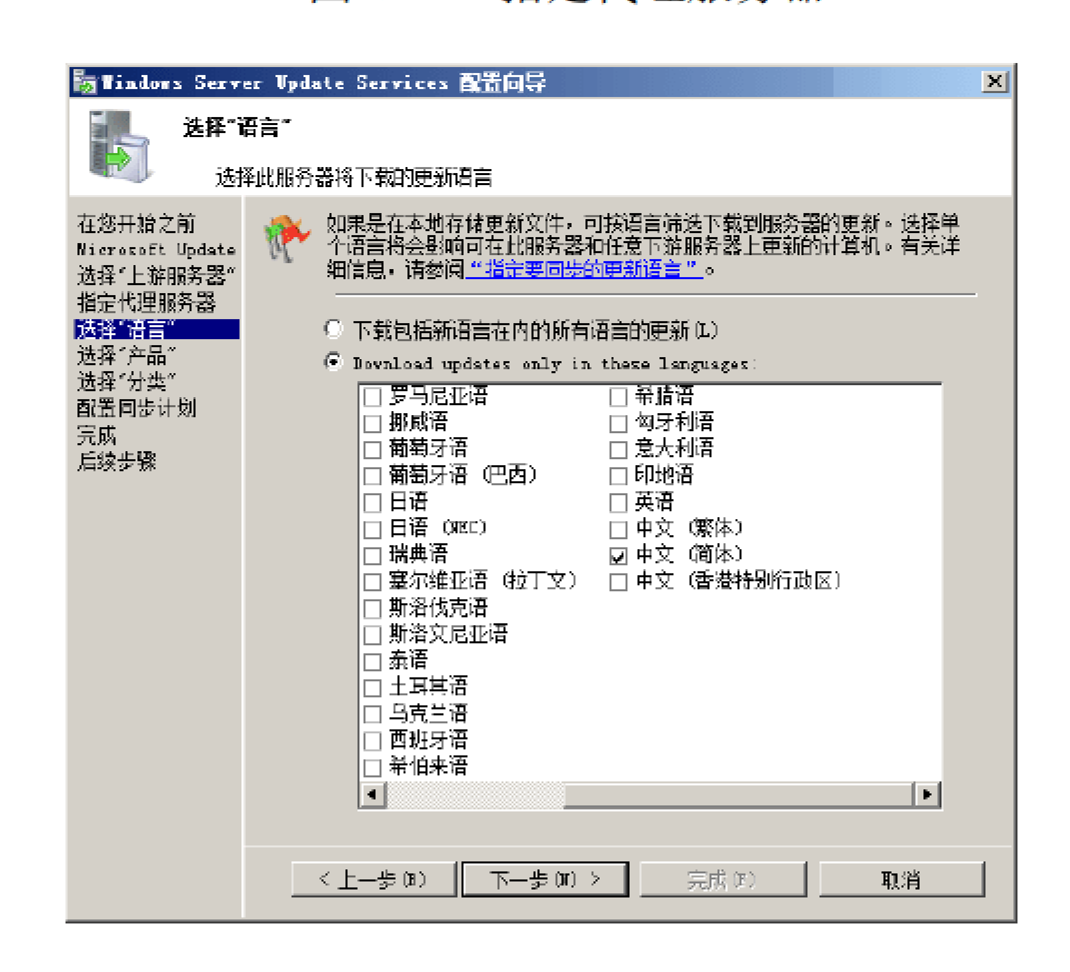


图 6-21　选择下载的更新语言

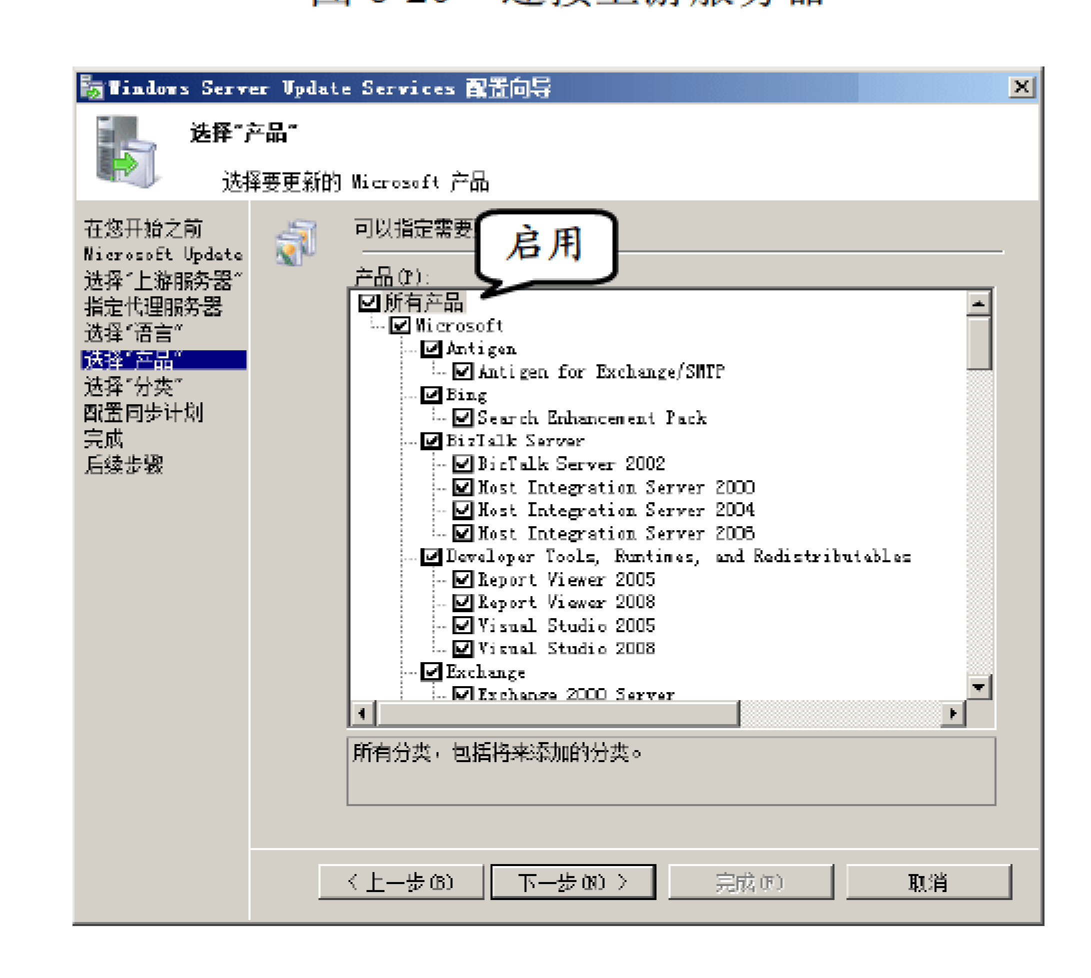


图 6-22　选择更新的产品

在【选择“分类”】对话框中，可以指定要同步的更新分类，如在此启用【所有分类】复选框，并单击【下一步】按钮，如图 6-23 所示。



图 6-23　选择分类

在【设置同步计划】对话框中，可以选中【手动同步】单选按钮，也可以选中【自动同步】单选按钮，并将同步时间选择在网络空间的时间段内，避免影响其他网络应用。然后，单击【下一步】按钮，如图 6-24 所示。

在【完成】对话框中，默认已经启用【启动 Windows Server Update Services 管理控制台】和【开始初始同步】复选框，此时，单击【下一步】按钮即可，如图 6-25 所示。

在【后续步骤】对话框中，用户可以查看到将 WSUS 服务器集成到环境中的后续步骤，这些后续步骤是可选的，管理员可以根据需要有

选择性地进行配置。此时，可以直接单击【完成】按钮即可，如图 6-26 所示。

WSUS 对客户端的管理都是通过分组的方式进行的，分组标准非常灵活，可以根据所需的更新类型划分，也可以根据所需部门进行划分，也可删除多余分组。在默认情况下，所有 WSUS 客户端都将存储在“未分配的计算机”分组中，管理员可以根据需要将其迁移或复制到其他分组。



图 6-24　设置同步计划

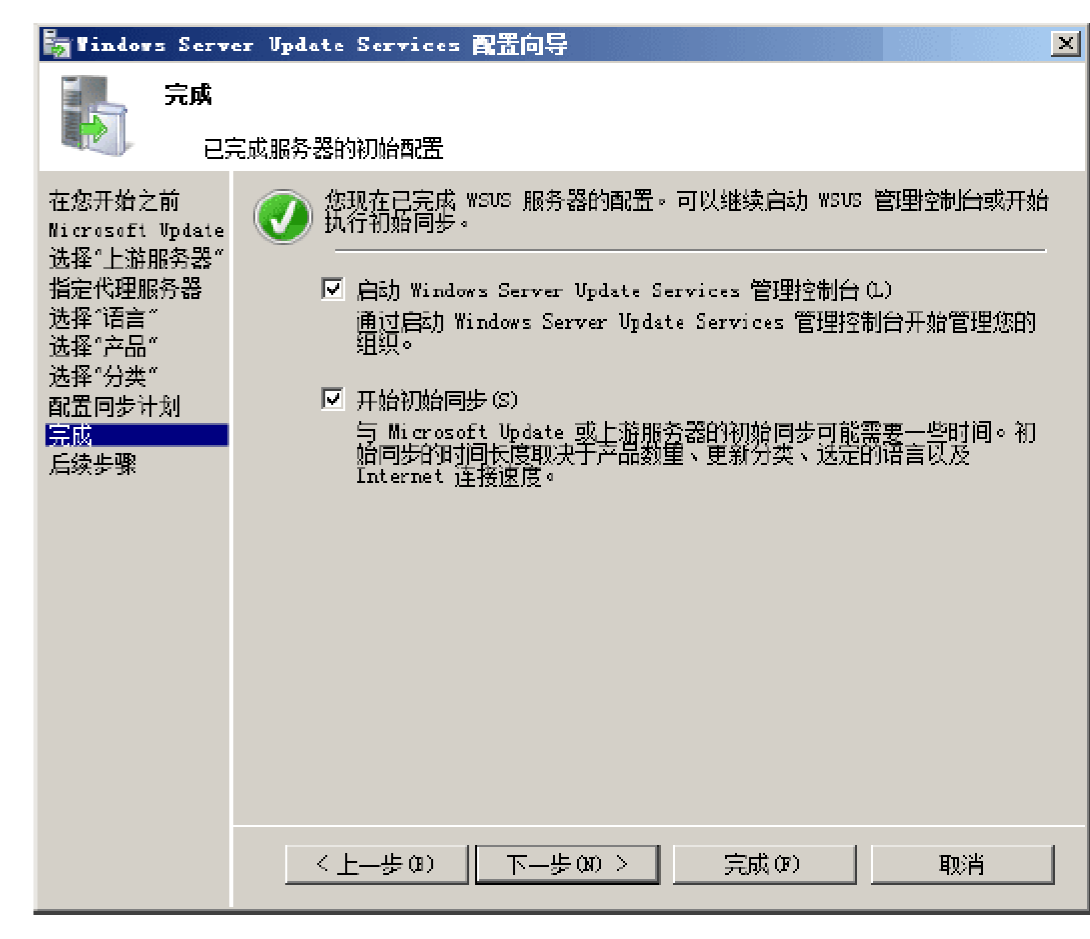


图 6-25　【完成】对话框

在正确配置 WSUS 客户端后，服务器将自动发现这些客户机，并显示在【未分配的计算机】列表中，如图 6-27 所示。如果没有立即显示，可以按 F5 键，或者单击【菜单栏】内【查看】按钮，执行【刷新】命令，尝试刷新一下服务器。

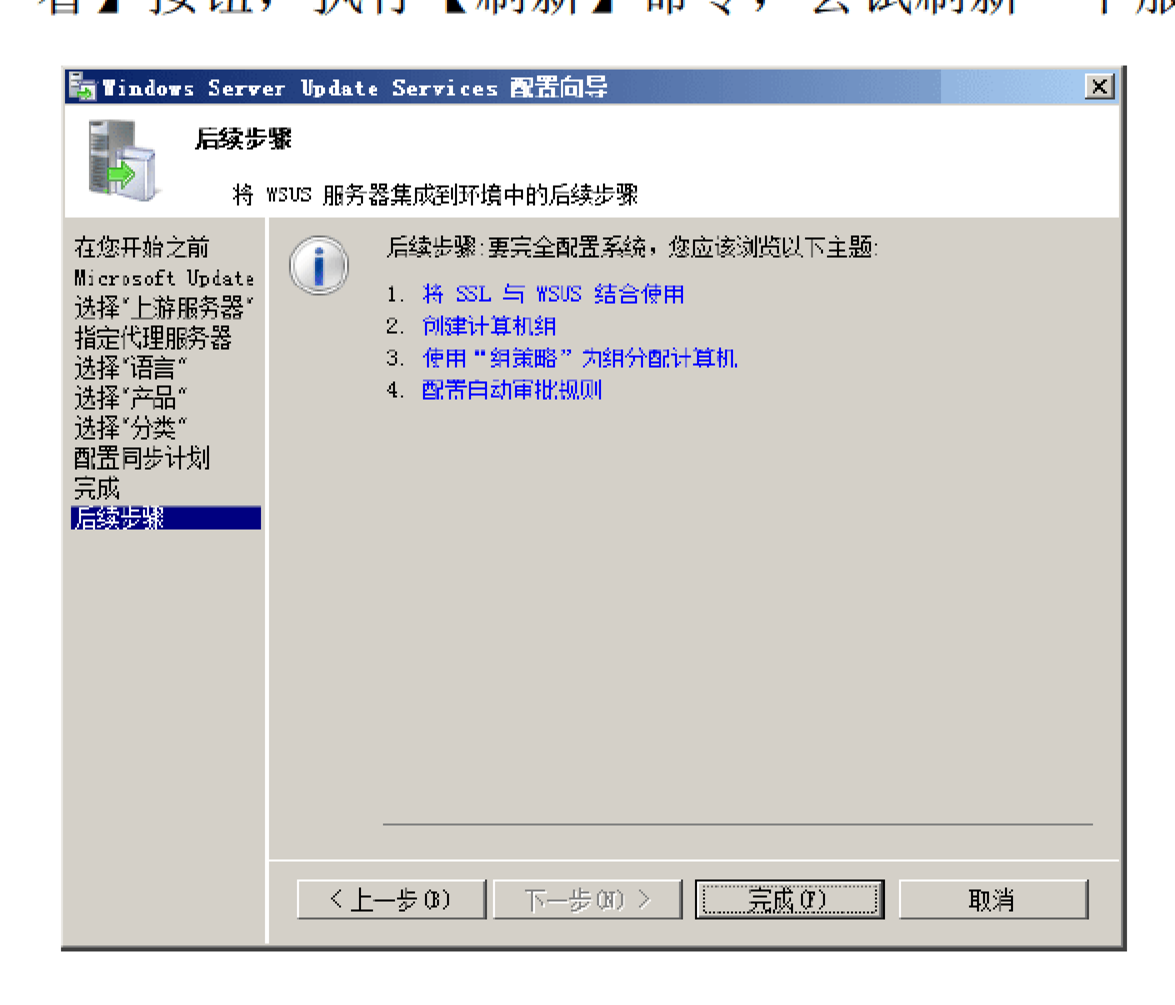


图 6-26　配置完成



图 6-27　Update Service 窗口

6.4.3　配置 WSUS 客户端

凡是具备自动更新功能的 Windows 操作系统，都可以配置为 WSUS 客户端。根据计算机

所在网络环境采取不同的配置方法。在域环境中，可以使用组策略对象（GPO）完成；在工作组环境中，可以使用本地组策略对象或者直接修改注册表完成。

如果通过组策略为 Active Directory 网络中的计算机指定 WSUS 升级服务器地址，需要在包括网络中所有计算机的“组织单元”或其上一级“组织单元”中配置组策略，或者将需要更新的计算机移动到一个新创建的“组织单元”中，然后再对该组中的所有计算机进行操作。

在此，将所有的计算机添加到指定的组织单位（test）中，然后，执行【开始】|【管理工具】|【组策略管理】命令，在打开的窗口中，依次展开【林】|【域】|slkj.com 节点，右击 test 选项，并执行【在这个域中创建 GPO 并在此处链接】命令，如图 6-28 所示。

在【新建 GPO】对话框的【名称】文本框中，输入一个便于识别的名称，并单击【确定】按钮，如图 6-29 所示。

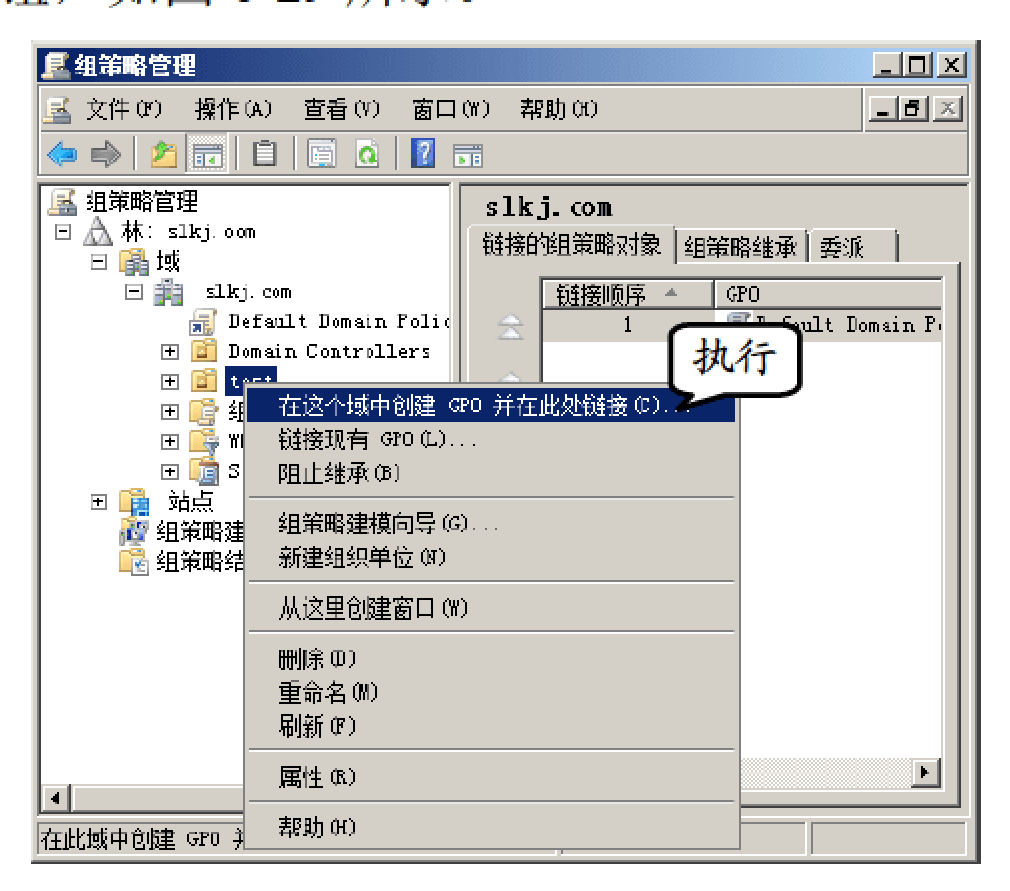


图 6-28 【组策略管理】窗口

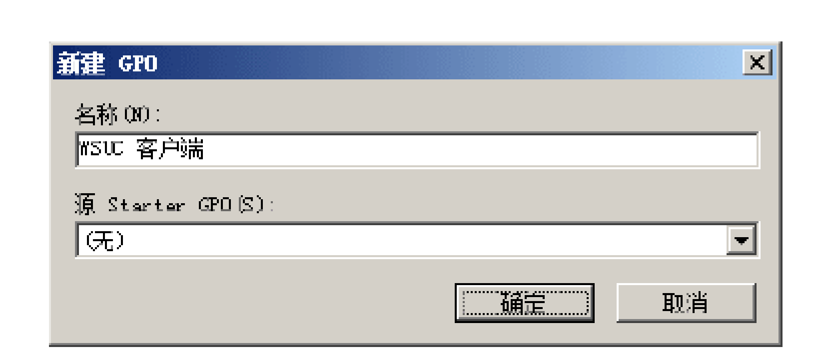
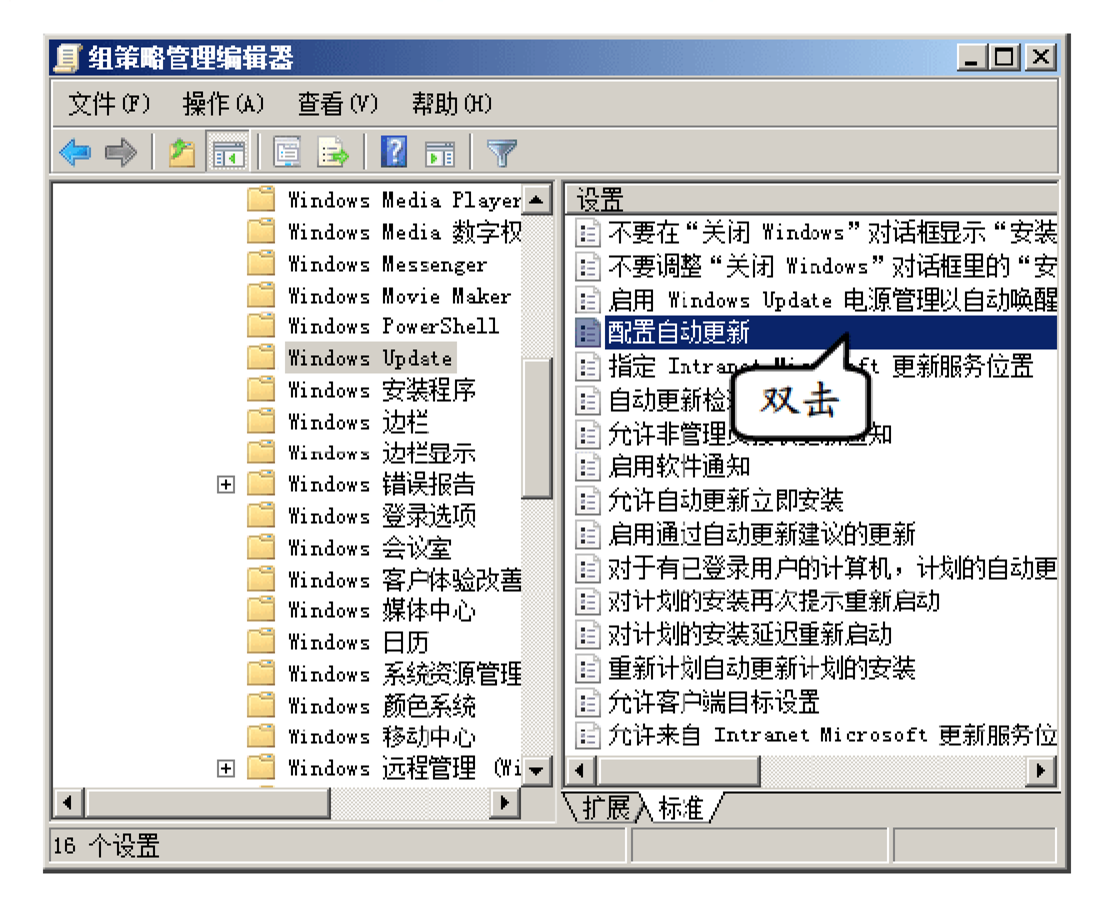


图 6-29 输入名称

右击新建的 GPO 并执行【编辑】命令，在打开的【组策略管理编辑器】窗口中，依次展开【计算机配置】|【策略】|【管理模板】|【Windows 组件】节点，选择 Windows Update 选项，在右侧窗格中，双击【配置自动更新】选项，如图 6-30 所示。

接着，在弹出的【配置自动更新 属性】对话框中，选中【已启用】单选按钮，然后，在【配置自动更新】右侧下拉列表中选择对应的自动更新类型，及根据需要还可以设置计划安装日期和时间，图 6-31 所示为默认设置。



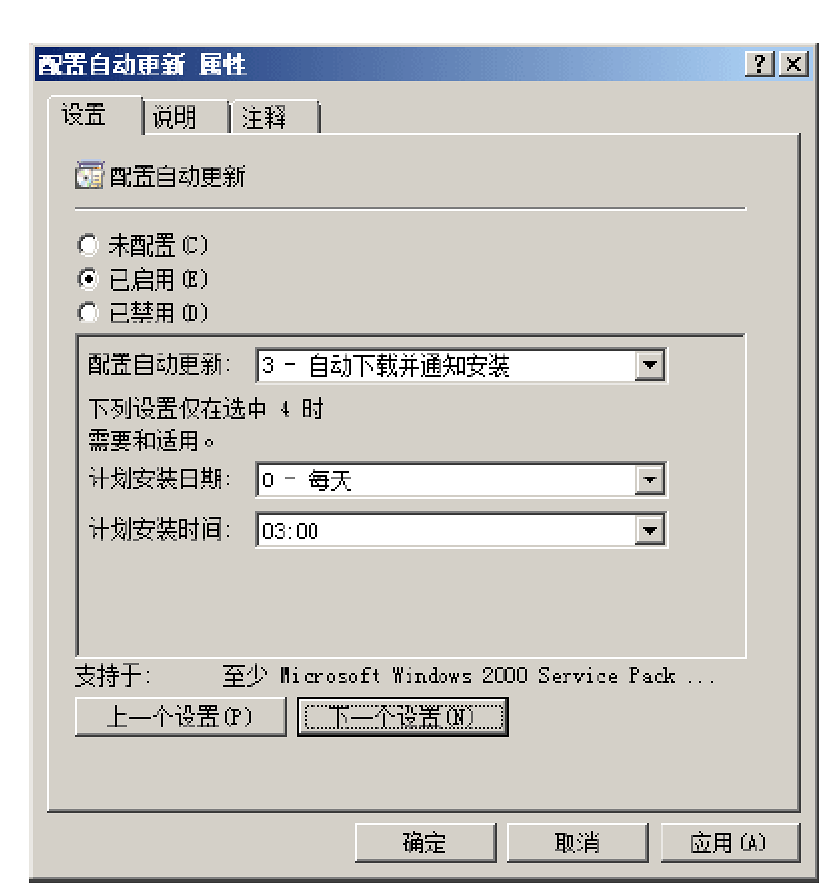


图 6-30 【组策略管理编辑器】窗口

图 6-31 启用自动更新

单击【下一个设置】按钮，在【指定 Intranet Microsoft 更新服务位置 属性】对话框中，选中【已启用】单选按钮，并在【设置检测到更新的 Intranet 更新服务】和【设置 Intranet 统计服务器】（用于获取客户端的状态和需求信息）文本框中输入相应内容，如图 6-32 所示。然后，依次单击【应用】和【确定】按钮。

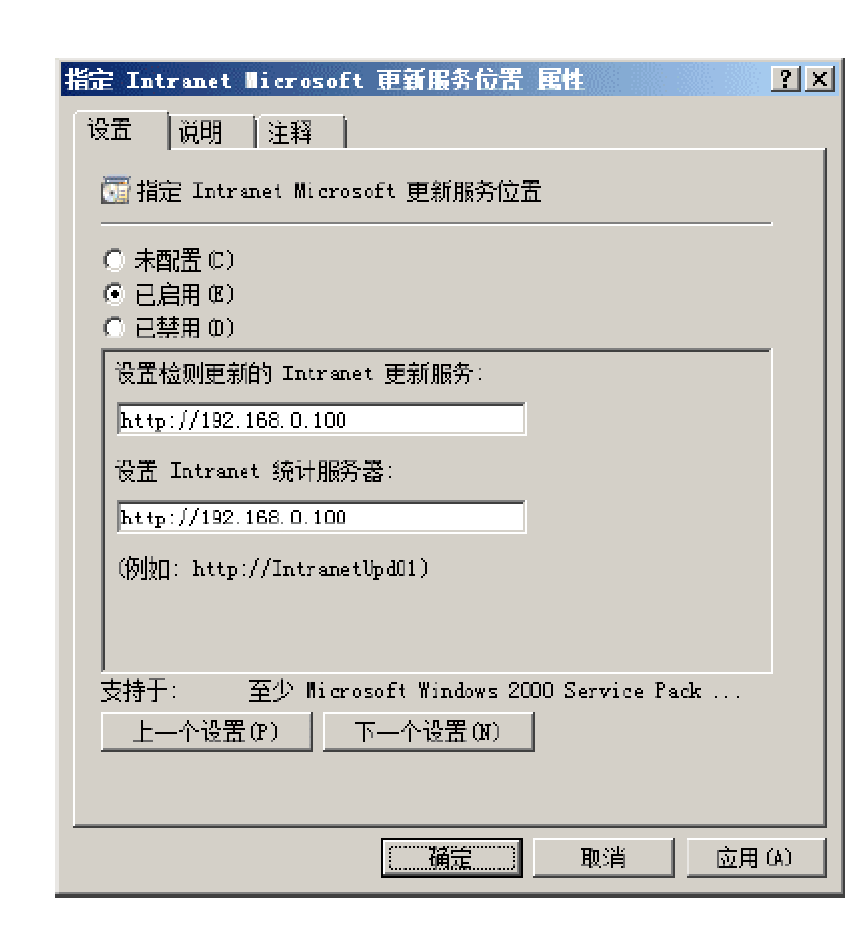


图 6-32　指定 Intranet Microsoft 更新服务器

由于组策略的刷新和应用需要一定的时间，所有保持编辑结果后即使客户端重新登录到域控制器也可能无法立即联系到 WSUS 服务器。而在默认情况下，每隔 90min 计算机组策略便会在后台刷新一次，刷新的时间可能随机偏移 0～30min，客户端计算机在域控制器刷新组策略 20min 后才可以应用到组策略。

6.4.4　网管心得——漏洞修补方略

大多数蠕虫病毒都是通过系统漏洞进行传播的，同时网络扫描和利用系统漏洞，也是“黑客”最常用的攻击手段之一。因此，为保护网络的安全性，必须做好漏洞补丁的安装管理工作。

对于普通用户来讲，系统漏洞修补主要是安装官方网站公布的补丁程序，但是对于服务器或者是网络中大规模的补丁部署，通常是一项非常重要的工作。在安装补丁程序之前，必须先在实验环境中进行测试和分析，然后才可以在网络中大规模部署。

1. 环境分析

用户只有在真正了解网络的内部状况后，才能够有效地实施漏洞修补。例如，及时掌握网络资产情况、设备运行状况，包括网络运行的设备型号、厂商、操作系统的种类及版本等。另外，还要了解企业的主要业务系统及其重要数据，根据需要划分安全等级，以确定补丁的紧急程度和修补时间。

2. 补丁分析

用户的计算机系统信息、硬件等设备的变化，都可能导致无法正确安装官方发布的系统漏洞补丁，甚至在安装后导致一系列其他问题。因此，部署之前一定要针对用户系统环境进行测试，切不可盲目地安装补丁，否则将带来许多意想不到的问题，包括如下几个方面。

- ❑ 导致系统兼容性出现问题，甚至不能使用。
- ❑ 系统崩溃，无法正常工作。
- ❑ 系统部分功能无法使用。

在得到补丁之后，正确的做法如下所述。

- ❑ 在测试环境中，测试对业务系统的影响以及兼容性。

- ❑ 了解补丁自身的稳定性。
- ❑ 查看补丁是否还存在其他漏洞。
- ❑ 在大规模部署之前，进行小范围的短时间的联机测试。在测试过程中，应做好详细的测试记录，了解补丁程序和其他相关组件对象之间的兼容性，对原有系统功能的影响，是否可以卸载，是否可以“回滚”等。

3. 分发安装

对于网络用户而言，管理员可以通过组策略、Windows Server Update Services（WSUS）等多种方法，将已获得的系统补丁分发到客户端。其中，WSUS 为微软公司提供的专用于补丁更新的服务组件，可以根据客户端的实际情况，自动将补丁程序分发到用户的计算机中。

6.5 操作实例二

6.5.1 操作实例——漏洞评估扫描工具

X-Scan 采用多线程方式对指定 IP 地址进行安全漏洞检测，能够针对已知漏洞，给出相应的漏洞报告和准确的解决方案。

1. 实例目的

- ❑ 发现系统漏洞。
- ❑ 扫描系统开放服务。
- ❑ 扫描系统弱口令。

2. 实例步骤

（1）在 X-Scan 文件夹目录下，双击 X-Scan_gui.exe 应用程序图标，如图 6-33 所示。
（2）在该软件主界面中，单击【设置】菜单，并执行【扫描参数】命令，如图 6-34 所示。

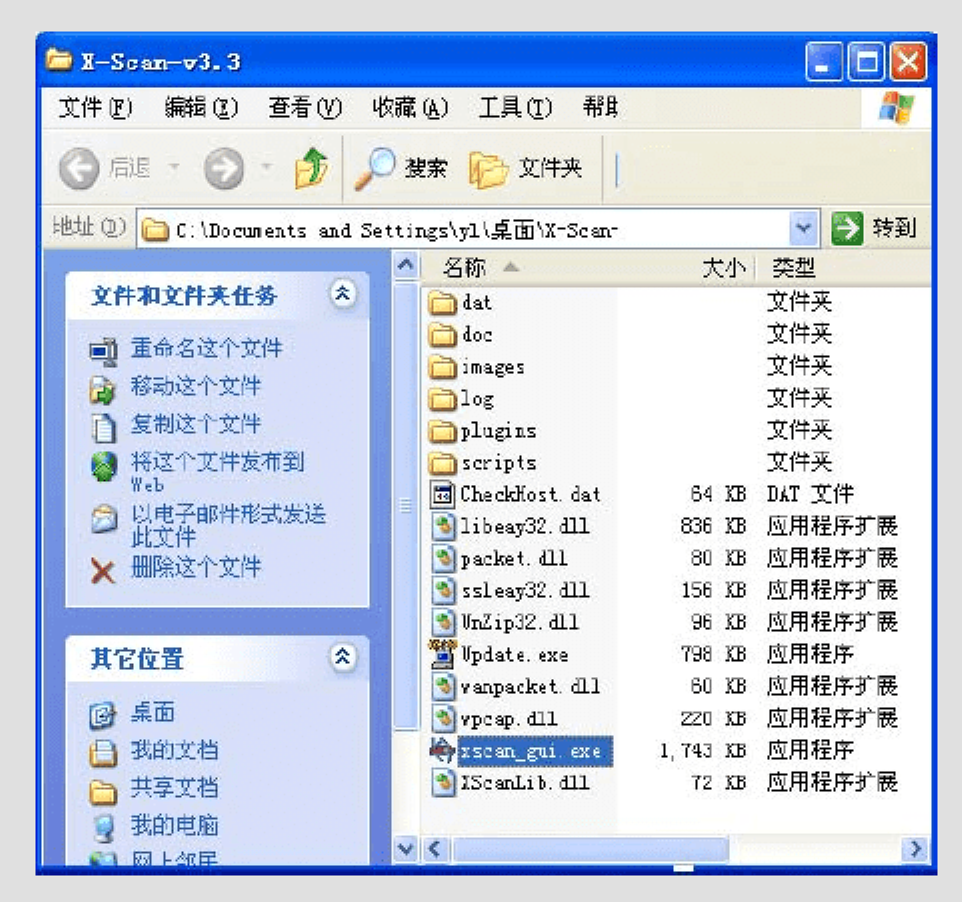


图 6-33　X-Scan 文件夹目录

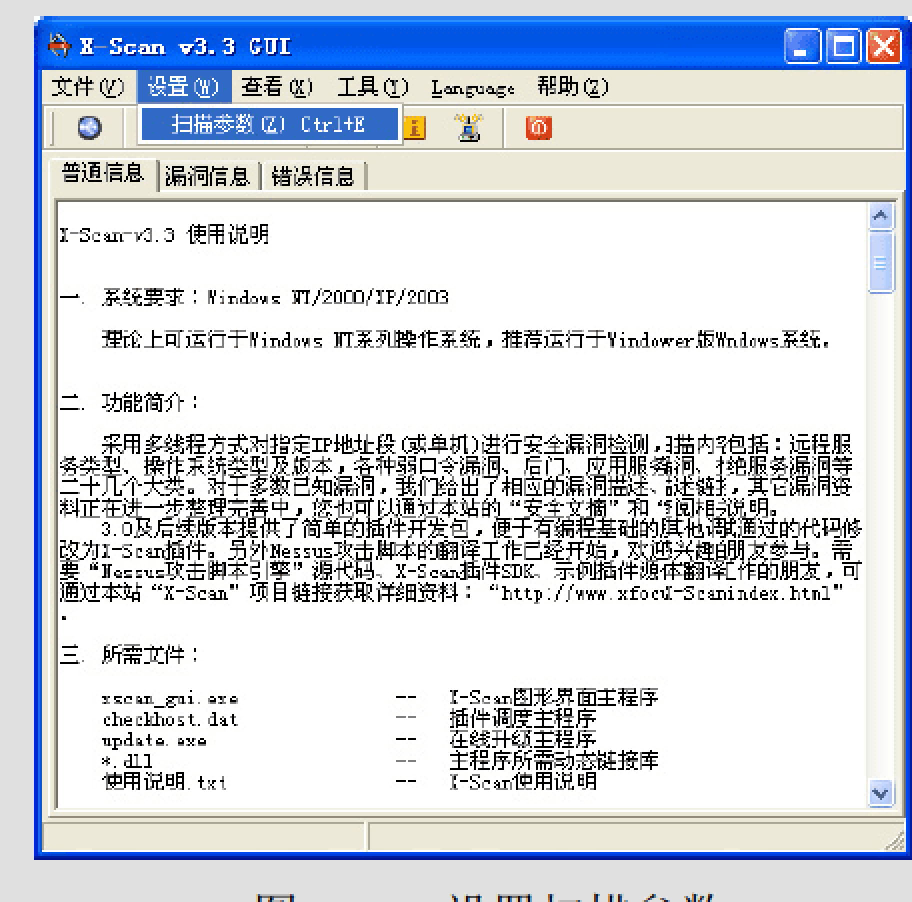


图 6-34　设置扫描参数

（3）在弹出的【扫描参数】窗口的右侧【指定 IP 范围】文本框内，输入 IP 地址（如“192.168.0.2”），如图 6-35 所示。

（4）在【扫描参数】窗口中，展开【全局设置】节点，并选择【扫描模块】选项，然后启用相关扫描项，如图 6-36 所示。

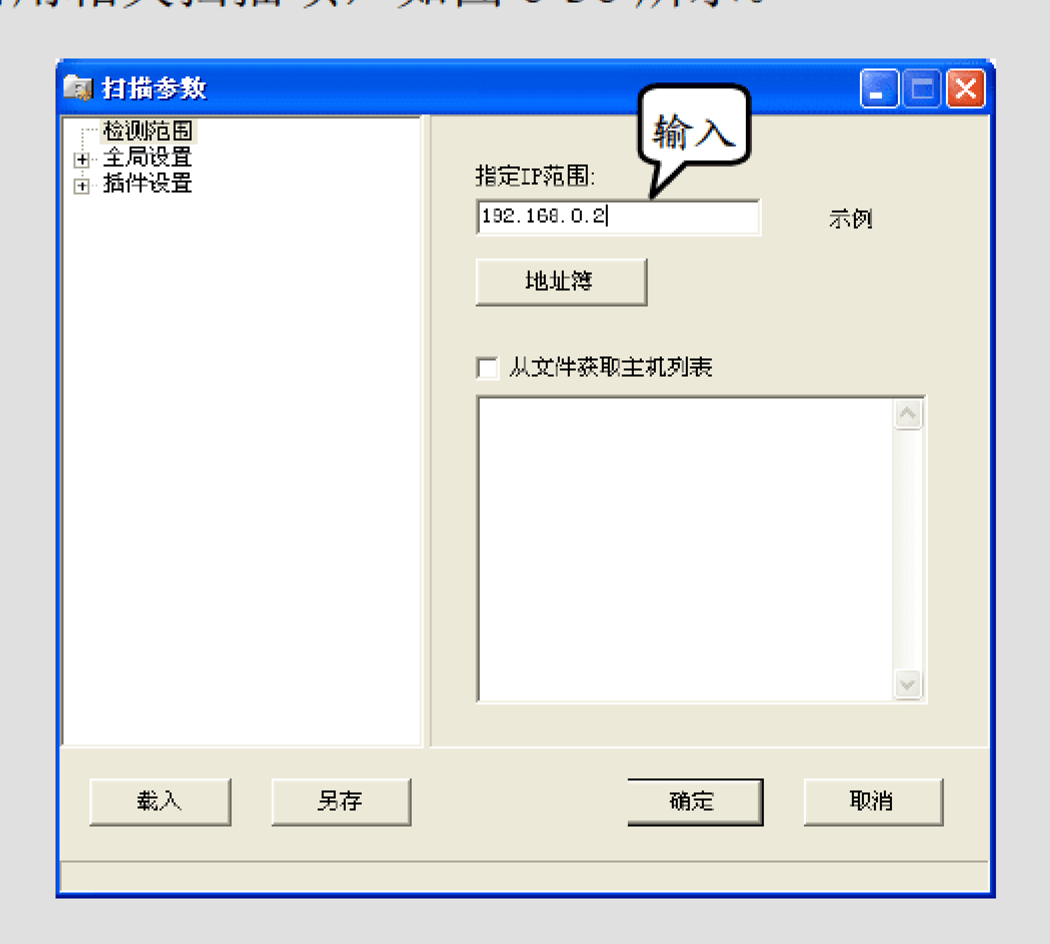


图 6-35　输入扫描 IP 范围



图 6-36　启用扫描项

（5）选择该菜单下【并发扫描】选项，输入最大并发主机数量（10），最大并发线程数（100），如图 6-37 所示。

（6）选择该菜单下【扫描报告】选项，在【报告文件】文本框中输入文件名，如“text.html”，启用【扫描完成自动生成并显示报告】复选框，如图 6-38 所示。

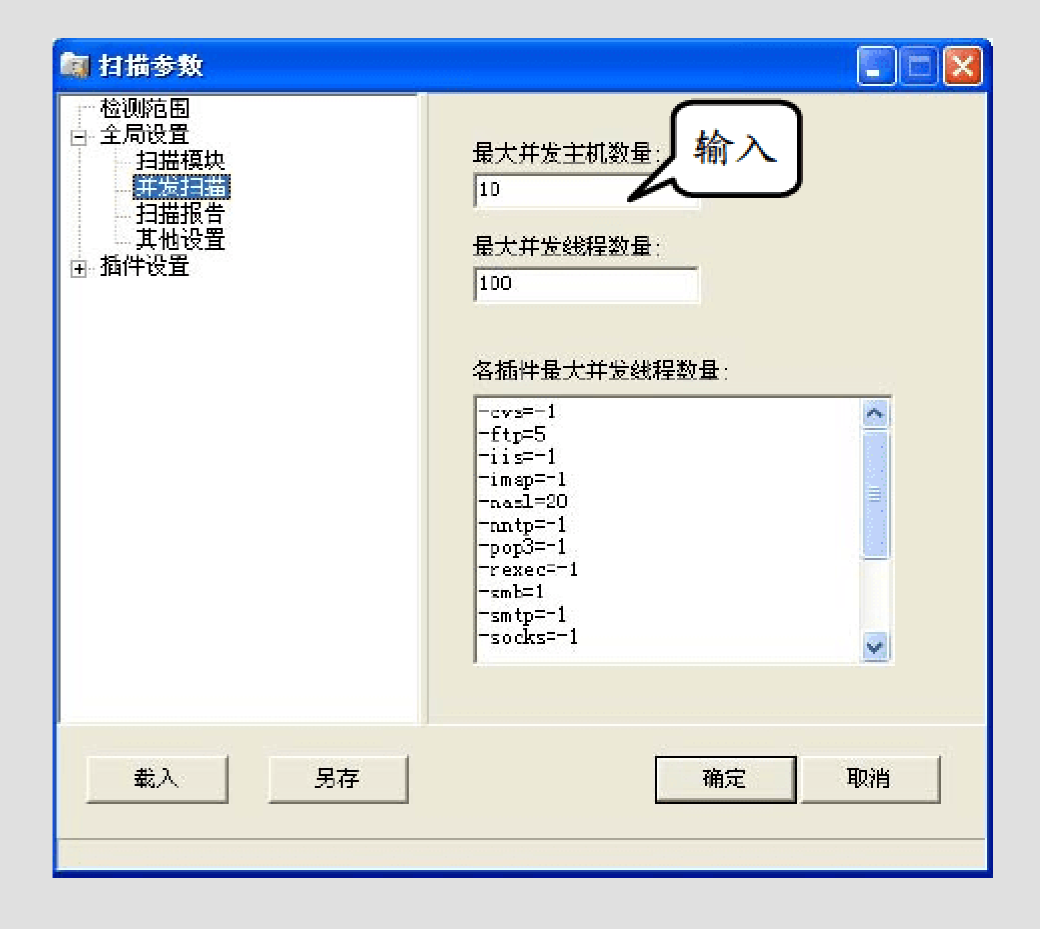


图 6-37　并发扫描采用默认设置

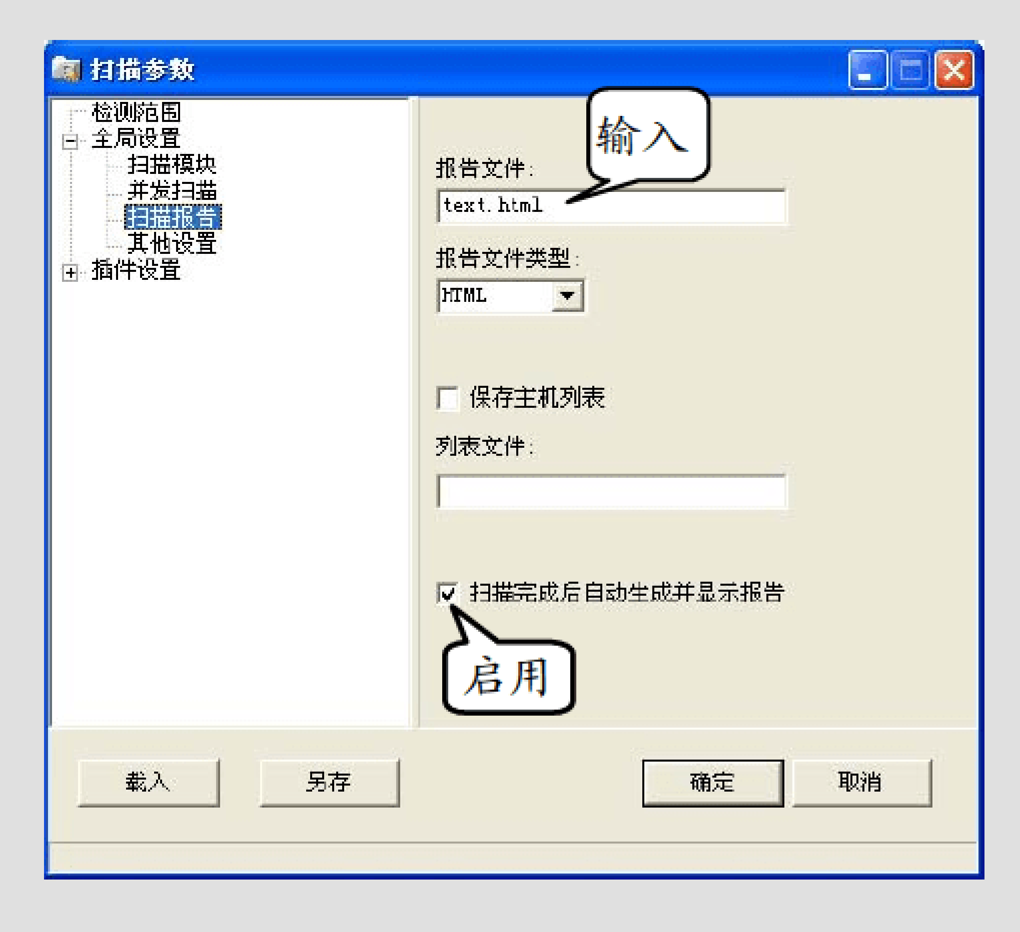


图 6-38　文件类型为 HTML

（7）选择该菜单下【其他设置】选项，启用【跳过没有检测到开放端口的主机】和【使用 NMAP 判断远程操作系统】复选框，并单击【确定】按钮，如图 6-39 所示。

（8）在 X-Scan v3.3 GUI 窗口的工具栏中，单击【启动】按钮，如图 6-40 所示。

（9）当扫描完成时，查看扫描报告如图 6-41 所示。



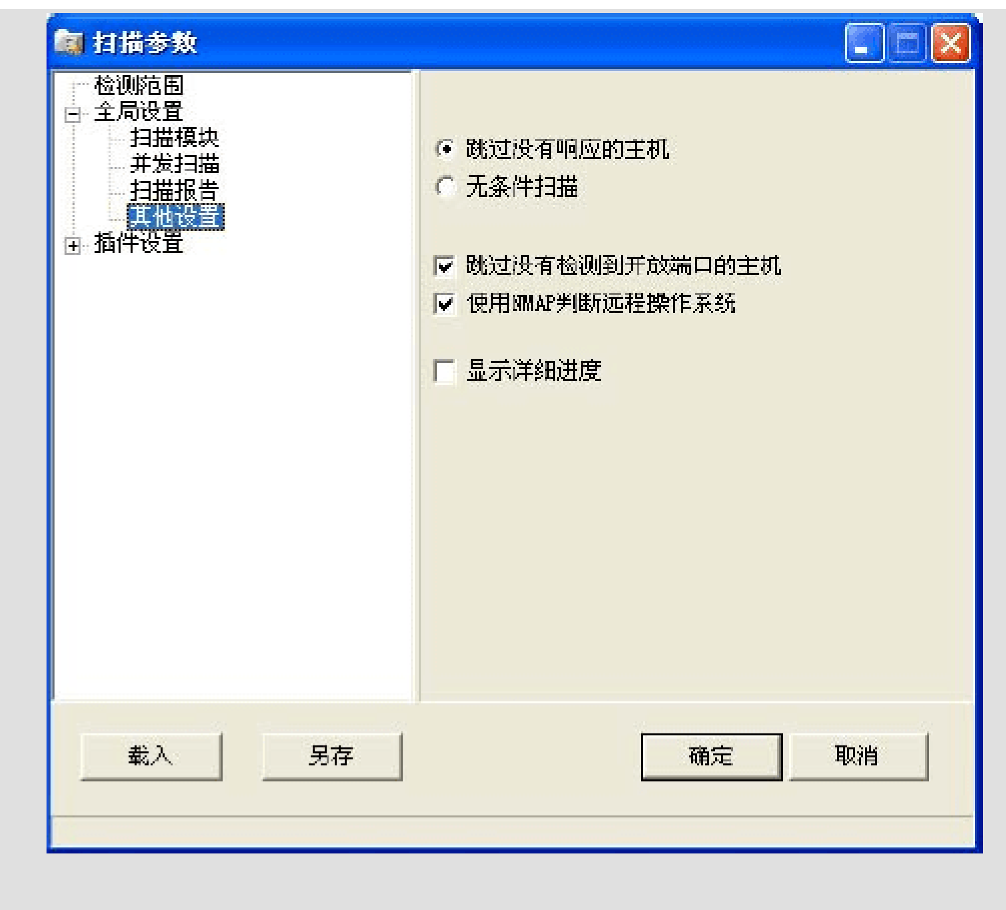
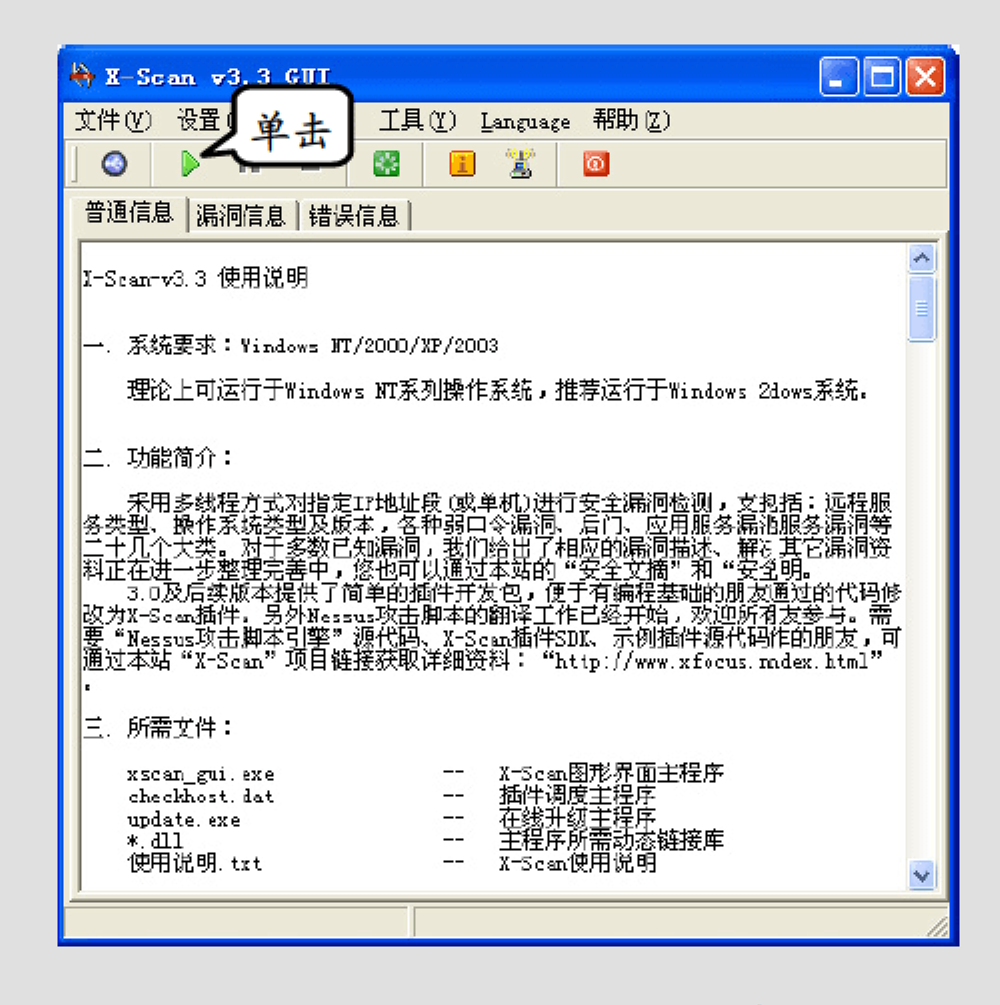


图 6-39 【扫描参数】窗口



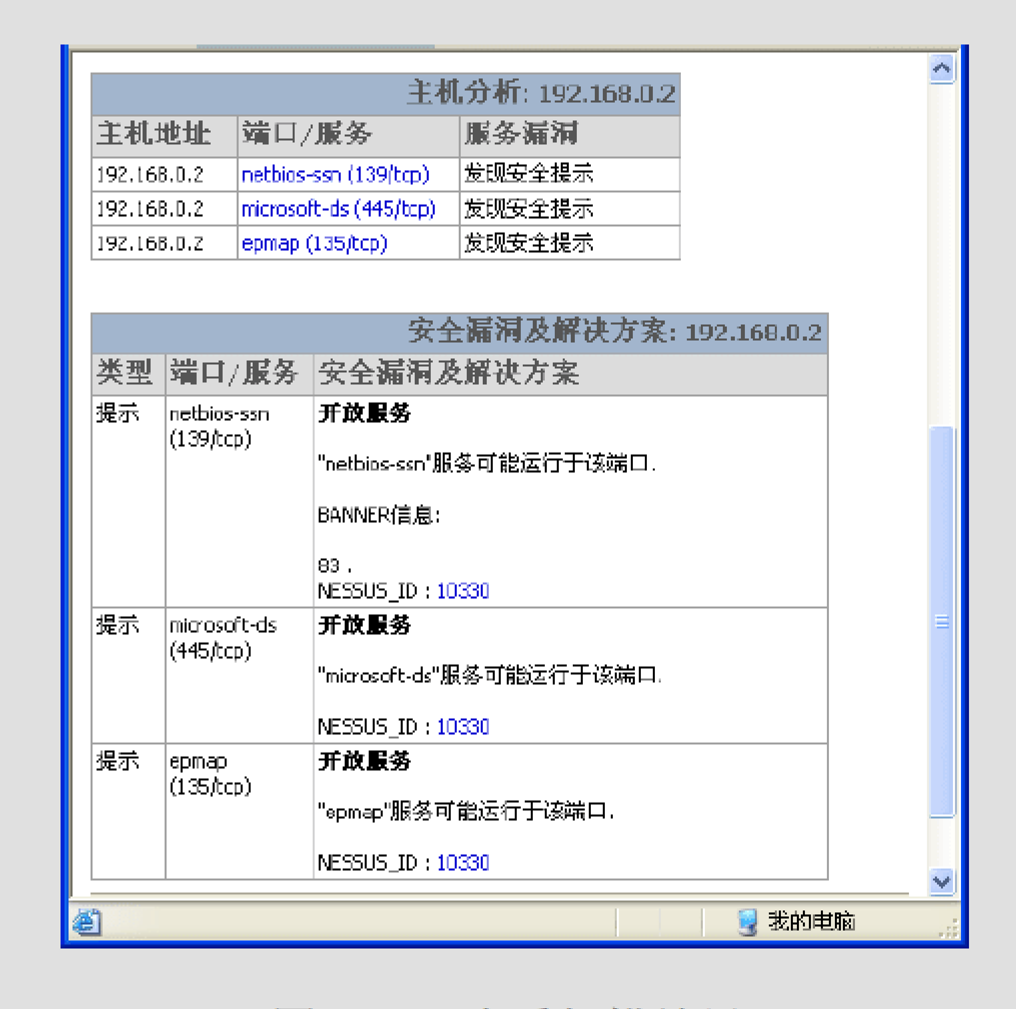


图 6-40 X-Scan v3.3 GUI 窗口

图 6-41 查看扫描结果

6.5.2 操作实例——漏洞评估扫描工具安装

漏洞扫描工具通过对系统进行动态的试探和扫描，发现系统潜在的弱点、不合理配置等问题，根据漏洞扫描结果提供的线索，建议采取相应的补救措施或自动填补某些漏洞。

1. 实例目的

- ❑ 接受软件协议。
- ❑ 设置安装路径。

2. 实例步骤

（1）在桌面双击 Setup_Fluxay5.exe 程序图标，如图 6-42 所示。

（2）在弹出的【许可证协议】窗口中，单击【我接受】按钮，如图 6-43 所示。

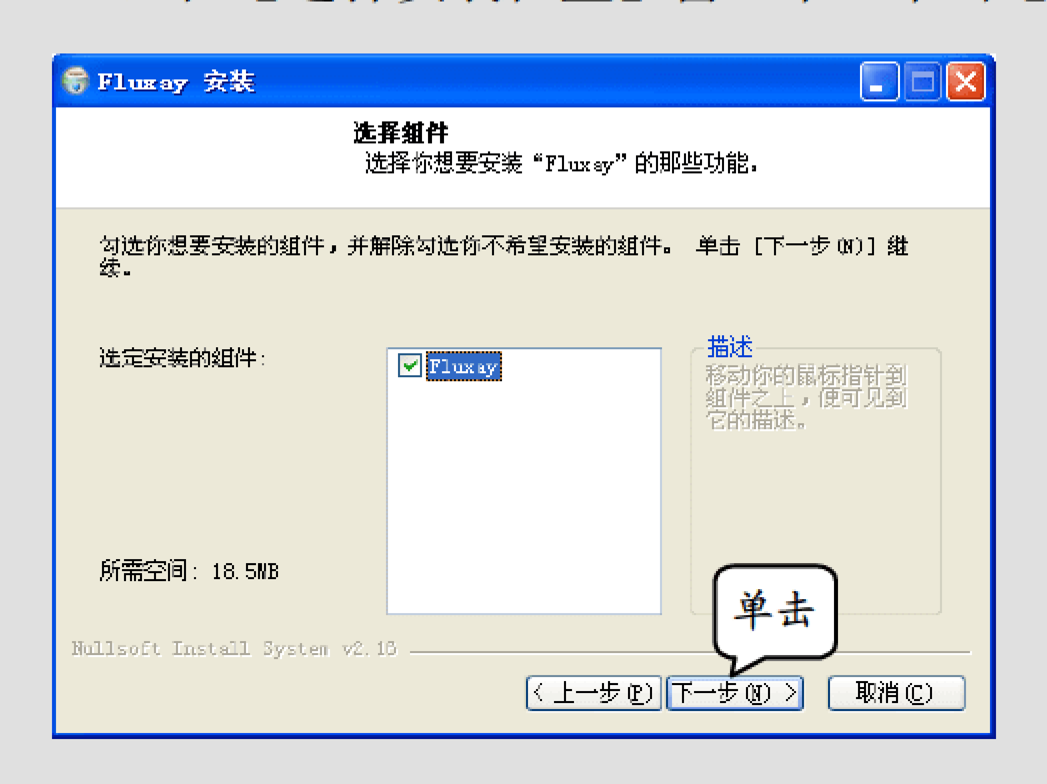


图 6-42 执行应用程序

图 6-43 【许可证协议】窗口

（3）在【选择组件】窗口中，单击【下一步】按钮，如图 6-44 所示。

（4）在【选择安装位置】窗口中，单击【浏览】按钮，如图 6-45 所示。



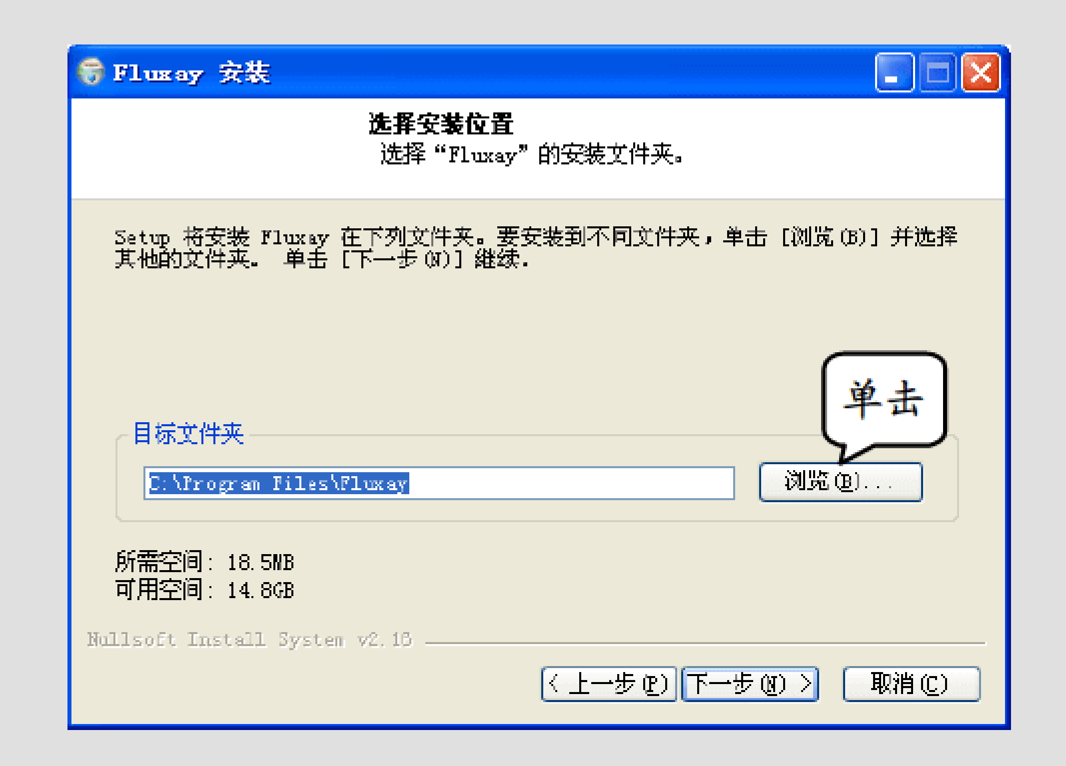


图 6-44 【选择组件】窗口

图 6-45 【选择安装位置】窗口

（5）在弹出的【浏览文件夹】对话框中，选择【本地磁盘（F:）】选项，并单击【确定】按钮，如图 6-46 所示。

（6）在【选择安装位置】窗口中，单击【下一步】按钮，如图 6-47 所示。



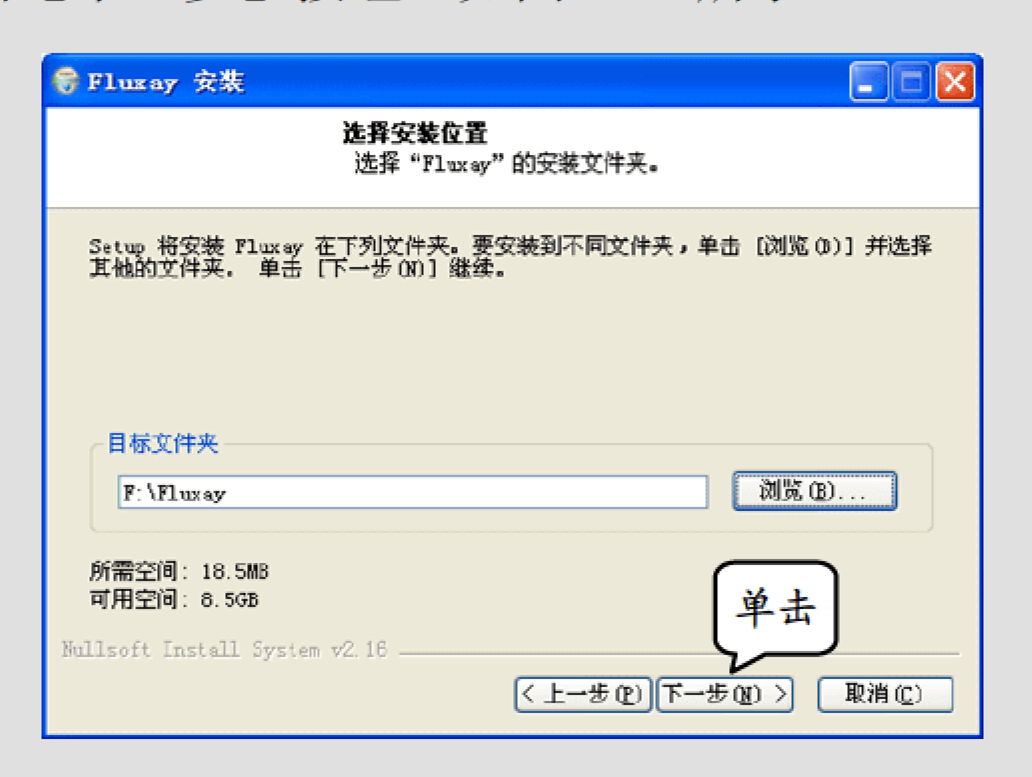


图 6-46 【浏览文件夹】对话框

图 6-47 选择安装路径

（7）在【选择"开始菜单"文件夹】窗口中，单击【安装】按钮，如图 6-48 所示。

（8）在弹出的 RegSvr32 对话框中，单击【确定】按钮，如图 6-49 所示。

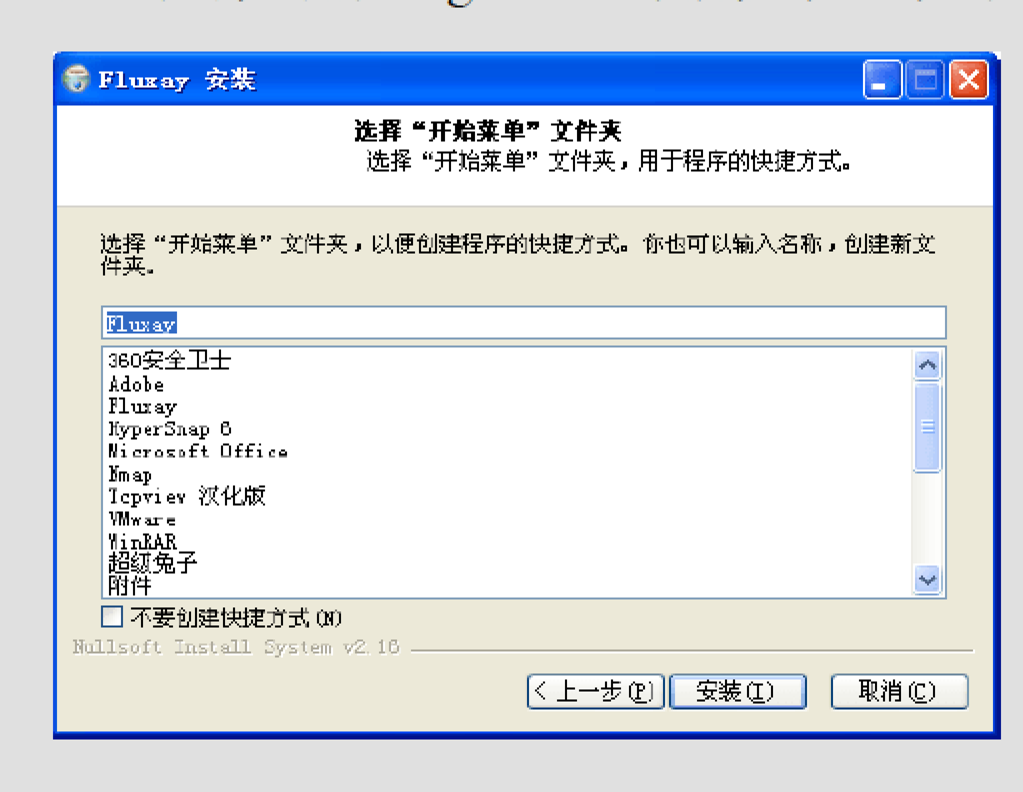



图 6-48　选择“开始菜单”文件夹

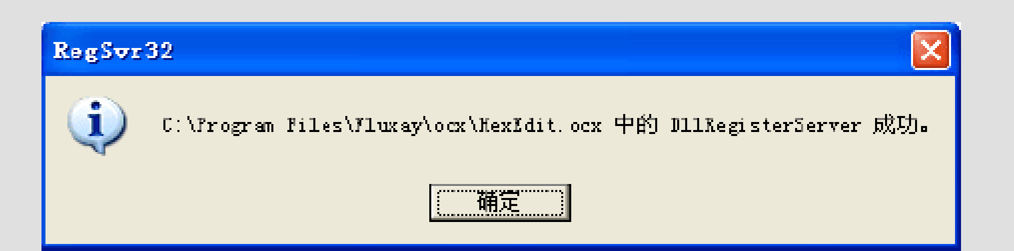


图 6-49　RegSvr32 对话框

第三篇　网络设备安全

第 7 章 交换机安全配置

在交换机上进行安全配置，使其成为安全性加强的交换机，具有抗攻击性，比普通交换机（不进行任何设置）具有更高的智能性和安全保护功能。在系统安全方面，交换机在网络由核心到边缘的整体架构中实现了安全机制，即通过特定技术（如风暴控制、流控制、保护端口等）对网络管理信息进行传输控制；在接入安全性方面，采用安全接入机制，包括 IEEE 802.1x 接入验证、RADIUS 等技术。

除了具备一般功能外，安全性加强的交换机还具备普通交换机所不具备的安全策略功能。从网络安全和用户业务应用出发，可实现特定的安全策略、限制非法访问、进行事后分析、有效保障用户网络业务的正常开展等功能，从而更好地遏制了随着网络应用而泛滥的内网安全隐患。

本章以基于端口的各种传输控制技术、PVLAN 技术、IEEE 802.1x 认证技术和远端网络监控技术对交换机进行安全配置。

本章学习要点：

- 掌握基于端口的传输控制
- 了解及掌握 PVLAN 安全配置
- 基于端口的 IEEE 802.1x 认证
- 配置 RMON

7.1 基于端口的传输控制

一般地，交换机都具有基于端口的传输控制功能，能够实现风暴控制、端口保护和端口安全等。传输控制功能用于交换机与交换机之间在发生拥塞时通知对方暂时停止发送数据包。如广播风暴抑制可限制广播流量的大小，对超过设定值的广播流量进行丢弃处理。不过，交换机的传输控制只能对经过端口的各类传输进行简单的速率限制，将广播、组播的异常流量限制在一定的范围内，而无法区分流量是否正常。

7.1.1 风暴控制

当端口接收到大量的广播、单播或多播包时，就会发生广播风暴，并且转发这些数据包将导致网络速度变慢或超时。因此，借助于对端口的广播风暴控制，在某些数据包过量时，交换机会暂时禁止该类数据包的转发，直至数据流恢复正常，从而有效地避免硬件损坏或链

路故障导致的网络瘫痪。默认状态下，广播、多播和单播风暴控制被禁用。

1. 开启风暴控制

若要在交换机上，开启风暴控制，其语法格式为：

```
Switch(config-if)#storm-control {broadcast | multicast | unicast} level {level
[level-low] | bps bps [bps-low] | pps pps [pps-low]}
```

- **broadcast** 代表广播风暴；multicast 代表组播风暴；unicast 代表未知的单播风暴。
- **level** 指定阻塞端口的带宽上限值。当广播、多播或单播传输占到宽带的多大比例（百分比）时，端口将阻塞传输。取值范围为 0.00~100.00。如果将值设置为 100.00，将不限制任何传输；如果将值设置为 0.00，那么，该端口的所有广播、多播和单播都将被阻塞。
- **level-low** 指定启用端口的带宽下限值。该值应当小于或等于上限值，当广播、多播或单播传输占用带宽的比例低于该值时，端口恢复转发传输。取值范围为 0.00~100.00。
- **bps** 指定端口阻塞的传输速率上限值。当广播、多播或单播传输达到每秒若干比特（bps）时，端口将阻塞传输。取值范围为 0.0 ~ 10 000 000 000.0。
- **bps-low** 指定端口启用的传输速率下限值。该值应当小于或等于上限值，当广播、多播或单播传输低于每秒若干比特（bps）时，端口将恢复传输。取值范围为 0.0 ~ 10 000 000 000.0。
- **pps** 指定端口阻塞的转发速率上限值。当广播、多播或单播传输速率达到每秒若干数据包（pps）时，端口将阻塞传输。取值范围为 0.0 ~ 10 000 000 000.0。
- **pps-low** 指定端口启用的传输速率下限值。该值应当小于或等于上限值，当广播、多播或单播转发速率低于每秒若干数据包（pps）时，端口将恢复传输。取值范围为 0.0 ~ 10 000 000 000.0。

如果要在交换机的特定端口（如 fastethernet0/17 端口），将广播风暴级别限制在 70.5%，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/17
Switch(config-if)# storm-control broadcast level 70.5
Switch(config-if)# end
Switch# show storm-control fastethernet0/17 broadcast
Interface Filter State Level Current
----------- ------------- -------- --------
Fa0/17 Forwarding 70.50% 0.00%
Switch# copy running-config startup-config
```

另外，还可以设置风暴发生时交换机的处理方式，其语法格式如下所示。

```
Switch(config-if)# storm-control action {shutdown | trap}
```

默认状态下，将过滤外出的传输，并不发送 SNMP 陷阱。选择 shutdown 关键字，在风暴期间将禁用端口；选择 trap 关键字，当风暴发生时，产生一个 SNMP 陷阱，向网络管理软件

发出警报。

2. 禁用风暴控制

当在交换机上，禁用风暴控制功能时，只需在开启此功能的命令前添加“no”，如在交换机的 fastethernet0/17 端口禁用广播风暴控制功能和风暴控制处理方式时，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/17
Switch(config-if)# no storm-control broadcast level
Switch(config-if)# no storm-control action shutdown
Switch(config-if)# end
Switch# show storm-control fastethernet0/17 broadcast
Interface  Filter  State  Level  Current
Switch# copy running-config startup-config
```



利用 show storm-control fastethernet0/17 broadcast 命令，显示并校验该接口当前的配置；copy running-config startup-config 命令保存当前配置。

7.1.2　流控制

在千兆端口启用流控制后，可以在拥塞期间暂停与其他终端的连接。也就是说，当端口处于拥塞状态，无法接收到数据流时，将通知其他端口暂停发送，直到恢复正常状态。例如，本地一台交换机发现任何终端发生拥塞时，它将发送一个暂停帧，以通知其连接伙伴或远端拥塞设备。当这些设备收到暂停帧后，将停止发送数据包，以防止在拥塞期内丢失。但流控制只适用于交换机的 1000Base-T（快速以太网端口）、1000Base-SX（多模光纤接口）和 GBIC（Giga Bitrate Interface Converter，千兆光纤接口）端口。

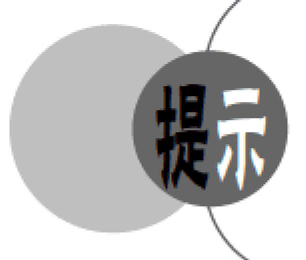
若要在交换机上，对特定端口进行流量控制配置时，所采用的命令格式如下所示。

```
Switch(config-if)# flowcontrol {receive | send} {on | off}
```

- **receive**　指定流量控制中接受暂停帧。
- **send**　指定流量控制中发送暂停帧。
- **on**　开启流量控制功能。
- **off**　禁用流量控制功能。

例如，在交换机特定端口（如 GigabitEthernet4/4 端口），开启接受暂停帧的流量控制功能，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet4/4
Switch(config-if)#flowcontrol receive on
Switch(config-if)#end
Switch# copy running-config startup-config
```



若要关闭流控制中发送暂停帧功能，可选用“off”参数，同样还可以开启或关闭发送暂停帧功能。另外，当在交换机配置有 QoS（Quality of Service）时，不要再配置 IEEE 802.3x 流控制。

7.1.3 保护端口

保护端口可以确保同一交换机上的端口之间不进行通信。因为保护端口不向其他保护端口转发任何单播、多播和广播包传输，要实现保护端口间的传输，都必须通过第三层设备转发。然而，保护端口与非保护端口间的传输不受任何影响。

在交换机上，把某端口设置为保护端口，其语法格式如下所示。

```
Switch(config-if)# switchport protected
```

例如，将交换机的 fastethernet1/1 端口设置为保护端口，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport protected
Switch(config-if)#end
Switch# copy running-config startup-config
```

7.1.4 端口阻塞

交换机的默认操作中，未知目标 MAC 地址的广播数据包将被允许从端口向外传输，但如果未知的单播和多播通信被转发到保护端口，将导致安全问题。此时，可以采用阻塞端口的方式，防止未知的单播和多播通信在端口间转发。

在交换机特定端口上，禁用未知多播和未知单播从某端口向外转发，其命令格式分别如下所示。

```
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
```

- block 表示未知数据包。
- multicast 表示多播数据包。
- unicast 表示单播数据包。

例如，在交换机的 fastethernet1/1 端口，禁用未知多播和未知单播从某端口向外转发，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport block multicast
```

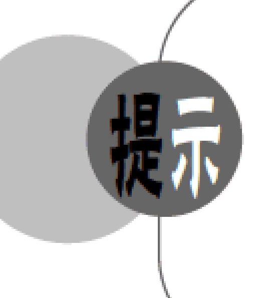
```
Switch(config-if)# switchport blockunicast
Switch(config-if)#end
Switch# copy running-config startup-config
```

7.1.5　端口安全

借助端口安全设置，可以只允许指定的MAC地址或指定数量的MAC地址访问某个端口，从而避免未经授权的计算机接入网络，或限制某个端口所连接的计算机数量，从而确保网络接入的安全。

当配置端口安全时，应当注意以下问题。

- 安全端口不能是Trunk端口。
- 安全端口不能是Switch Port Analyzer （SPAN）的目的端口。
- 安全端口不能是属于EtherChannel的端口。
- 安全端口不能是Private VLAN端口。



EtherChannel特性在交换机到交换机、交换机到路由器之间提供冗余的、高速的连接方式，简单说就是将两个设备间多条快速以太网或吉比特以太网物理链路捆在一起组成一条设备间逻辑链路，从而达到增加带宽，提供冗余的目的。

1．配置安全端口

在交换机上进行安全端口配置时，可依次进行启用该端口的安全功能、在端口设置安全MAC地址的最大数量、违反规则后的处理模式、指定安全MAC地址和启动Sticky learning几项操作，其语法格式分别如下所示。

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum value
Switch(config-if)# switchport port-security violation {restrict | shutdown}
Switch(config-if)# switchport port-security mac-address mac_address
Switch(config-if)# switchport port-security mac-address sticky
```

- **安全MAC地址最大数量设置**

在端口设置安全MAC地址的最大数量，以限制该端口所连接的计算机数量。取值范围为1～3072，默认值是1。

- **违反规则后处理模式的设置**

设置违反规则后的处理模式，那么在安全违例事件发生时，会将端口置于restrict（限制）或shutdown（禁用）模式。选择restrict模式时，当非法MAC地址或太多MAC连接至该接口时，将丢弃数据包，并向网管计算机发送SNMP陷阱通知；选择shutdown模式时，发生安全错误的端口将被置于error-disable状态，除非网络管理员使用no shutdown命令手工激活，否则该端口失效。

❑ **指定安全 MAC 地址**

为端口指定安全 MAC 地址，也可以使用该命令指定最大安全 MAC 地址数。如果指定的 MAC 地址数量少于安全地址的最大数量，动态学习的 MAC 地址将被保留。

❑ **启动 Sticky learning**

在端口启用粘性学习（Sticky learning）功能，端口将把所有的动态安全 MAC 地址（包括启用粘性学习前动态获悉的安全 MAC 地址）转换为粘性安全 MAC 地址，并把它们加入到运行配置中。

然而，粘性安全 MAC 地址不会自动加入到交换机重启时使用的启动配置文件中。如果将粘性安全 MAC 地址保存到启动配置文件中，则交换机重启后接口无需重新获悉这些地址。如果不保存配置，这些 MAC 地址将丢失。如果禁用了粘性学习，粘性安全 MAC 地址将转换为动态安全地址，并从运行配置中删除。安全端口可以有 1～132 个相关联的安全地址，而整个交换机最多可以有 1024 个安全地址。

例如，在交换机的 fastethernet1/1 端口，设置安全 MAC 地址的最大数量为 5、违反规则后置于 restrict 模式、指定安全 MAC 地址为 000a.6e0c.902b 并启用 Sticky 功能，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address 000a.6e0c.902b
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)#end
Switch# copy running-config startup-config
```

2. 设置端口安全老化

当为端口指定最大 MAC 地址数时，为了保障该端口能够得以充分利用，可以采用设置端口安全老化时间和模式的方式，让系统能够自动删除长时间未连接的 MAC 地址，从而使管理员不必手动删除，减少网络维护的工作量。

在交换机上设置端口安全老化时间和模式的方式，其语法格式如下所示。

```
Switch(config-if)# switchport port-security [ aging time aging_time | type
{absolute | inactivity}]
```

❑ aging time aging_time 用于设置端口安全老化时间，取值范围为 0~1440 分钟。

❑ absolute，采用 absolute 模式，一旦到达指定的老化时间，那么立即会将 MAC 地址从安全地址列表中移除。

❑ inactivity，采用 inactivity 模式，即使到达指定的老化时间，如果没有其他数据通信，那么，MAC 地址仍然被保留在安全地址列表中。

例如，在交换机的 fastethernet1/1 端口，通过以下命令可以将端口安全老化时间和模式分别设置为 10 分钟和 inactivity。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)#switchport port-security aging time 10 type inactivity
Switch(config-if)#end
Switch# copy running-config startup-config
```


7.1.6　传输速率限制

网络传输速率变慢主要由于某些用户对网络流量的滥用。当使用 MRTG 等流量监控软件检测到流量来源于某个端口时，可以在核心交换机、汇聚交换机，甚至接入交换机上，对相应的端口作必要的处理，限制其传输带宽，从而限制每个用户所允许的最大流量，以便使其他网络用户能够恢复正常的网络应用服务。

在交换机上，配置端口带宽控制，其语法格式如下所示。

```
Switch(config-if)# rate-limit {input | output} [access-group acl-index] bps
burst-normal burst-max conform-action conform-action exceed-action exceed-
action
```

- input/output 表明在输入和输出方向应用该带宽限制。通常应当进行双向限制。
- access-group acl-index 用于定义使用该带宽限制的访问列表。
- bps 用于定义限制带宽，以 bps 为单位，并采用 8kbps 增量方式。
- burst-normal 用于定义所允许的普通突发速率。
- burst-max 用于定义所允许的最大突发速率。
- conform-action conform-action 用于指定在规定最大带宽时所执行的操作，通常为 transmit，即允许发送。
- exceed-action exceed-action 则用于指定在规定最大带宽时所执行的操作，通常为 drop，即丢弃。

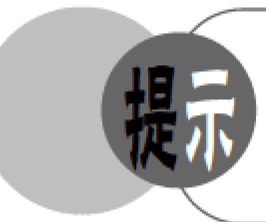
例如，限制交换机的 GigabitEthernet4/4 端口带宽为 128kbps，当连接的普通突发速率、最大突发在 8kBytes（即 64kbps）至 9kBytes（即 72kbps）范围内时，所执行的操作是 transmit（传输即发送）；当超出该范围时，则执行的相应操作为 drop。其中，128000 用于限制最大带宽，8000 和 9000 则用于限制突发连接，保证不因个别用户的大量传输而使整个链路性能大幅度下降。限制输入和输出速率后，可进行如下配置。

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet4/4
Switch(config-if)#ip access-group 120 in
Switch(config-if)#ip access-group 120 out
Switch(config-if)#rate-limit input access-group 120 128000 8000 9000 conform-
action transmit exceed-action drop
Switch(config-if)#rate-limit output access-group 120 128000 8000 9000 conform-
action transmit exceed-action drop
```

```
Switch(config-if)#end
Switch# copy running-config startup-config
```

配置中，应用的 IP 访问列表只需设置使用带宽限制的用户 IP 地址范围（192.168.0.0～192.168.255.255）即可，内容如下所示。

```
Switch(config)#access-list 120 permit ip 192.168.0.0 0.0.255.255 any
```

为了实现交换机快速执行流量分配操作，在启用宽带限制之前，必须先在全局模式下执行 ip cef 命令，启用交换机的快速转发技术。

7.1.7 MAC 地址更新通知

MAC 地址唯一地标识了世界上的每个以太网设备，每一个生产网络设备的厂商都要将 MAC 地址预先写进其设备中（如以太网网卡、路由器、交换机等）。目前来讲，获得 MAC 地址的方法有很多。这里主要以 Cisco 的 IOS 为例来讲解一下用户该如何获得、改变 MAC 地址，并使用 MAC 地址进行网络通信的过滤。

1. 获得 MAC 地址

在交换机中，可以通过 show mac-address-table 命令，来获取 MAC 地址表。

例如，Switch# show mac-address-table

```
Mac Address Table
-------------------------------------------
Vlan  Mac Address  Type Ports
------ ----------------- --------------
All  0014.1c40.b080  STATIC CPU
All  0100.0ccc.cccc  STATIC CPU
All  0100.0ccc.cccd  STATIC CPU
All  0100.0cdd.dddd  STATIC CPU
1  000f.1fd3.d85a  DYNAMIC Fa0/14
```

另外，还可以通过查看交换机端口信息，来获取 MAC 地址，其语法格式如下所示。

```
Switch#show interfaces
```

例如：Switch# show interfaces

```
Ethernet0/0 is up, line protocol is up
Hardware is AmdP2, address is 0003.e39b.9220 (bia 0003.e39b.9220)
Internet address is 1.1.1.1/8
```

输出显示中第二行，可看到“bia 0003.e39b.9220”，bia 即“烧录地址”（burned in address），MAC 地址即 0003.e39b.9220。

2. 改变 MAC 地址

更改 MAC 地址实质上为 MAC 欺骗，特别是对于无线网络的攻击，改变 MAC 地址是常用的方法。另外，改变 MAC 地址也可以用于合法的用途，如测试 MAC 过滤。

若要在交换机设备上，更改 MAC 地址，其语法格式如下所示。

```
Switch(config-if)#mac-address mac_address
```

例如，Switch#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet1/1
Switch(config-if)# mac-address 0000.0000.0001
Switch(config-if)#exit
```

完成 MAC 地址更改后，可以使用 show interface 命令来查看新的地址。

```
Switch#show interface fastethernet1/1
Ethernet0/0 is up, line protocol is up
Hardware is AmdP2, address is 0000.0000.0001 (bia 0003.e39b.9220)
Internet address is 1.1.1.1/8
```

3. 基于 MAC 地址的通信过滤

通过协议分析仪，可以发现网络中某些设备在执行非法的数据通信。例如，某设备通过多个 IP 地址发送数据包。这种情况，可以使用 show mac-address-table 命令来查看它所使用的交换机端口，并可以关闭此端口。但是，如果此端口连接的是一个集线器，而集线器又连接了许多其他设备时该怎么办？

此时，可使用 MAC 地址过滤来对交换机或路由器的数据通信进行过滤。

例如，Switch#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mac access-list extened filtermac
Switch(config-ext-macl)#deny host 0000.0000.0001 any
Switch(config-ext-macl)#permit any any
Switch(config-ext-macl)#exit
Switch(config)#interface GigabitEthernet1/0/40
Switch(config-if)#mac access-group filtermac in
Switch(config-if)#end
Switch# copy running-config startup-config
```

此配置是在 Cisco Catalyst 3750 GigabitEthernet Switch 交换机上完成。创建了一个名为“filtermac”的 ACL（访问控制表），该 ACL 拒绝了与源地址为 0000.0000.0001（十六进制非二进制）的所有数据通信，但是却允许其他地址的数据通信。然后，将这个 ACL 应用到交换机 GigabitEthernet1/0/40 端口，从而防止了拥有这个 MAC 地址的设备与本端口的数据通信，而不管它的 IP 地址是什么。

7.1.8 绑定 IP 和 MAC 地址

影响网络安全的因素很多，IP 地址盗用或地址欺骗就是其中一个常见且危害极大的因素。现实中，许多网络应用是基于 IP 的，比如流量统计、账号控制等都将 IP 地址作为标志用户的一个重要的参数。如果有人盗用了合法地址并伪装成合法用户，那么网络上传输的数据就可能被破坏，甚至盗用，造成无法弥补的损失。

针对目前 ARP 病毒肆虐，利用 ARP（地址解析协议）进行欺骗的网络问题也日渐严重。在防范过程中除了可以通过划分 VLAN 来抑制问题的扩散外，还可以将 IP 地址与 MAC 地址进行绑定以达到最佳的防范结果。

在交换机上简单实现 IP 地址与 MAC 地址绑定，实际上是使用端口（已配置过 IP 地址）来绑定 MAC 地址，即一个 MAC 地址与一个 IP 地址进行绑定，其语法格式如下所示。

```
Switch(config-if)#switchport port-security mac-address mac_address
```

- **mac_address** 代表被绑定的计算机 MAC 地址。

例如，若要将交换机的 fastethernet1/1 端口，与某计算机的 MAC 地址 000a.6e0c.902b 进行绑定，可进行如下配置。

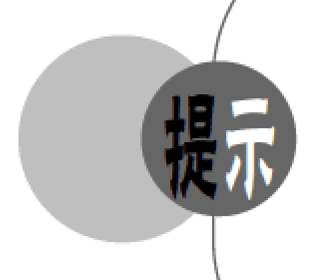
```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 000a.6e0c.902b
Switch(config-if)#end
Switch# copy running-config startup-config
```

这个配置只可以一个端口绑定一个 MAC 地址，少数人会用交换机一个端口只绑定一台计算机（浪费带宽）。通常要绑定多个 IP 地址与 MAC 地址，但必须首先创建两个访问控制列表（一个是关于 MAC 地址，一个是关于 IP 地址），然后将创建好的访问控制列表应用到需要配置的端口。

例如，在交换机上将某计算机的 MAC 地址 000a.6e0c.902b，和网络中所有能够访问该计算机的多台计算机，与交换机的 fastethernet1/1 端口（IP 地址为 10.0.0.1）进行绑定，即多个 IP 地址与 MAC 地址的绑定。可进行如下配置。

```
Switch# configure terminal
Switch(config)#mac access-list extended mac-vfast
Switch(config)#permit host 000a.6e0c.902b any
Switch(config)#permit any host 000a.6e0c.902b
Switch(config)# ip access-list extended ip-vfast
Switch(config)# permit ip 10.0.0.1 0.0.0.0 any
Switch(config)# interface Fa1/1
Switch(config)# mac access-group mac-vfast in
Switch(config)# ip access-group ip-vfast in
```

```
Switch(config-if)#exit
Switch# copy running-config startup-config
```

mac access-list extended mac-vfast 用来配置一个名称为 mac-vfast 的 MAC 访问控制列表；permit host 000a.6e0c.902b any 代表源 MAC 为 000a.6e0c.902b 的计算机可以访问网络中任意其他计算机；permit any host 000a.6e0c.902b 代表所有计算机可以访问目标 MAC 为 000a.6e0c.902b 的计算机；permit ip 10.0.0.1 0.0.0.0 any 表示允许 10.0.0.1 地址在网络内工作。

7.1.9 网管心得——第三层交换机技术白皮书

局域网交换机的引入，使得网络中计算机间可独享带宽，消除了无谓的碰撞检测和出错重发，从而提高了数据传输效率，因为在交换机中可并行地维护几个独立的、互不影响的通信进程。但是，当网络上某一节点发送广播或组播，或发送了一个交换机不认识的 MAC 地址封包时，交换机上的所有节点都将收到这一广播信息，那么整个交换环境构成一个大的广播域。点到点在数据链路层快速、有效地交换，但广播风暴会使网络的效率大打折扣。交换机的速度非常高，比路由器快得多，而且价格便宜得多。可以说，在网络系统集成的技术中，直接面向用户的第一层接口和第二层交换技术方面已得到令人满意的答案。

交换式局域网技术使专用的带宽为用户所独享，极大地提高了局域网数据传输的效率。但第二层交换也暴露出弱点，如对于广播风暴、异种网络互连、安全性控制等不能有效地解决。而此时，作为网络核心、起到网间互连作用的路由器技术也未出现质的突破。且大部分企业网都已变成实施 TCP/IP 协议的 Web 技术的内联网，用户数据越过本地的网络在网际间传送，因而，路由器常常不堪重负。另外，传统的路由器基于软件，协议复杂，与局域网速度相比，其数据传输的效率较低；同时它又作为网段（子网或 VLAN）互连的枢纽，这就使传统的路由器技术面临严峻的挑战。

在这种情况下，一种新的路由技术应运而生，即第三层交换技术，也称为 IP 交换技术、高速路由技术等。它是相对于传统交换概念而提出的，大都知道传统的交换技术是在 OSI 网络互联模型的第二层（数据链路层）应用的，而第三层交换技术则在网络模型中的第三层实现了数据包的高速转发。简单地说，第三层交换技术就是第二层交换技术+第三层转发技术，一种利用第三层协议中的信息来加强第二层交换功能的机制。

一个具有第三层交换功能的设备是一个带有第三层路由功能的第二层交换机，但它是两者的有机结合，并不是简单地把路由器设备的硬件及软件简单地叠加在局域网交换机上。从硬件的实现上看，目前，第二层交换机的接口模块都是通过高速背板/总线（速率可高达几十 Gbit/s）交换数据的，在第三层交换机中，与路由器有关的第三层路由硬件模块也插接在高速背板/总线上，这种方式使得路由模块可以与需要路由的其他模块间快速地交换数据，从而突破了传统的外接路由器接口速率的限制（10Mbit/s～100Mbit/s）。总体来讲，三层交换技术有以下技术特点。

1. 线速路由

和传统的路由器相比，第三层交换机的路由速度一般要快十倍或数十倍，能实现线速路由转发。传统路由器采用软件来维护路由表，而第三层交换机采用 ASIC（Application Specific Integrated Circuit）硬件来维护路由表，因而能实现线速的路由。



“线速”是网络设备交换转发能力的一个标准，而非通常所言的线速度和角速度。达到线速标准的设备，避免了非线速设备的转发瓶颈，称作“无阻塞处理”。

2. IP 路由

在局域网上，二层的交换机通过源 MAC 地址来标识数据包的发送者，根据目标 MAC 地址来转发数据包。对于一个目的地址不在本局域网上的数据包，二层交换机不可能直接把它送到目的地，需要通过路由设备（比如传统的路由器）来转发，这时就要把交换机连接到路由设备上。如果把交换机的默认网关设置为路由设备的 IP 地址，交换机会把需要经过路由转发的包送到路由设备上。路由设备检查数据包的目的地址和自己的路由表，如果在路由表中找到转发路径，路由设备把该数据包转发到其他网段上，否则，丢弃该数据包。专用（传统）路由器昂贵，复杂，速度慢，易成为网络瓶颈，因为它要分析所有的广播包并转发其中的一部分，还要和其他路由器交换路由信息，并且这些处理过程都是由 CPU 来处理的（不是专用的 ASIC），所以速度慢。第三层交换机既能像二层交换机那样通过 MAC 地址来标识转发数据包，又能像传统路由器那样在两个网段之间进行路由转发；而且由于是通过专用的芯片来处理路由转发，第三层交换机能实现线速路由。

3. 路由功能

比较传统的路由器，第三层交换机不仅路由速度快，而且配置简单。在最简单的情况（即第三层交换机默认启动自动发现功能时），一旦交换机接进网络，只要设置完 VLAN，并为每个 VLAN 设置一个路由接口。第三层交换机就会自动把子网内部的数据流限定在子网之内，并通过路由实现子网之间的数据包交换。管理员也可以通过人工配置路由的方式设置基于端口的 VLAN，给每个 VLAN 配上 IP 地址和子网掩码，就产生了一个路由接口。随后，手工设置静态路由或启动动态路由协议。

4. 路由协议支持

第三层交换机可以通过自动发现功能来处理本地 IP 包的转发及学习邻近路由器的地址，同时也可以通过动态路由协议 RIPv1，RIPv2，OSPF 来计算路由路径。路由信息协议（RIP）是一个内部网关协议（IGP），主要应用在中等规模的网络，采用距离向量算法，在路由信息中包括了到达目的 IP（向量）的跳跃次数（距离），跳跃次数最小的路径是最优路径。RIP 允许的最大跳跃次数为 15，需要跳跃 16 次及其以上的目的地址被认为是不可达的。RIP 路由器

通过周期性广播来与邻近的 RIP 路由器交换路由信息，广播的时间间隔可以设定。广播的内容就是整个路由表。当 RIP 路由器收到邻近路由器的路由表后，要经过计算来决定是否更新自己的路由表。如果自己的路由表需要更新，路由器在更新完毕后会立即把更新的内容发到邻近的路由器而不必等待广播间隔时间的结束。

5. 自动发现功能

一些第三层交换机具有自动发现功能，该功能可以减少配置的复杂性。第三层交换机可以通过监视数据流来学习路由信息，通过对端口入站数据包的分析，第三层交换机能自动地发现和产生一个广播域、VLAN、子网和更新它们的成员。自动发现功能在不改变任何配置的情况下，提高网络的性能。

第三层交换机启动后就自动具有 IP 包的路由功能，它检查所有的入站数据包来学习子网和工作站的地址，它自动地发送路由信息给邻近的路由器和第三层交换机，转发数据包。一旦第三层交换机连接到网络，它就开始监听网上的数据包，并根据学习到的内容建立并不断更新路由表。交换机在自动发现过程中，不需要额外的管理配置，也不会发送探测包来增加网络的负担。用户可以先用自动发现功能来获得简单高效的网络性能，然后根据需要来添加其他的路由、VLAN 等功能。

在第三层，自动发现有如下过程。

- 通过侦察 ARP，RARP 或者 DHCP 响应包的原 IP 地址，在几秒钟之内发现 IP 子网的拓扑结构。
- 在同一网络的不同网段之间建立一个逻辑连接，即在网段间进行路由，实现网段间信息通信。
- 学习地址，根据 IP 子网、网络协议或组播地址来配置 VLAN，使用 IGMP（Internet Group Management Protocol）来动态更新 VLAN 成员。
- 支持 ICMP（internet control message protocol ）路由发现选项。
- 存储学习到的路由到硬件中，用线速转发这些地址的数据包。
- 把目的地址不在路由表中的包送到网络上的其他路由器。
- 通过侦听 ARP 请求来学习每一台工作站的地址。
- 在子网之内实现 IP 包的交换。

7.2　PVLAN 安全

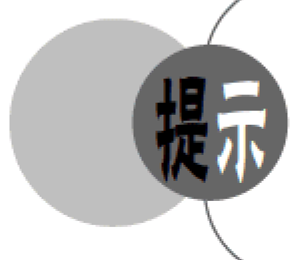
要在数据链路层网络上隔离用户或广播数据包，可以将一组设备加入到一个 VLAN 中，但 VLAN 的最大个数只有 4096，所以当需要隔离大量广播域时会受到 VLAN 个数的限制。例如，通常在服务提供商（SP）网络中，为了隔离不同客户之间的通信而将一个客户作为一个 VLAN，但如果客户数量增加到 VLAN 的最大个数时，服务提供商提供的服务将受到限制。

这种一个客户作为一个 VLAN 的解决方案，服务器提供商需要为每个客户分配一个子网的地址，不过会导致 IP 地址的浪费。此时，可利用 Private VLAN 技术来解决。

7.2.1 PVLAN 概述

随着网络的迅速发展，用户对于网络数据通信的安全性提出了更高的要求，诸如防范黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全性；传统的解决方法是给每个客户分配一个 VLAN 和相关的 IP 子网，通过使用 VLAN，每个客户从数据链路层被隔离开，可以防止任何恶意的行为和 Ethernet 的信息探听。然而，这种分配每个客户单一 VLAN 和 IP 子网的模型造成了巨大的可扩展方面的局限。这些局限主要有下述几个方面。

- **VLAN 的限制**　交换机固有的 VLAN 数目的限制。
- **复杂的 STP**　对于每个 VLAN，每个相关的 Spanning Tree 的拓扑都需要管理。
- **IP 地址的紧缺**　IP 子网的划分势必造成一些 IP 地址的浪费。
- **路由的限制**　每个子网都需要相应的默认网关的配置。



STP（Spanning Tree Protocol，生成树协议），该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

Private VLAN（私有 VLAN，PVLAN），能够为相同 VLAN 内的不同端口提供隔离的 VLAN。也就是说，通过 PVLAN 技术可以隔离相同 VLAN 中网络设备之间的流量，并且位于相同子网的所有设备都只能与网关或其他网络进行通信，实现网络内部的隔离。

PLAN 可以将一个 VLAN 的广播域划分为多个子域，每个子域都由 Primary VLAN（主 VLAN）和 Secondary VLAN（辅助 VLAN）一对 VLAN 组成。在整个 PVLAN 域中，只有一个主 VLAN，每个子域有不同的辅助 VLAN，并通过辅助 VLAN 实现数据链路层网络的隔离。

- **主 VLAN**　主 VLAN 是 PVLAN 的高级 VLAN。
- **辅助 VLAN**　辅助 VLAN 是 PVLAN 中的子 VLAN，并且映射到一个主 VLAN。每台接入设备都连接到辅助 VLAN。

辅助 VLAN 有如下两种类型。

- **隔离 VLAN（Isolated VLAN）**　同一个隔离 VLAN 中的端口相互不能进行数据链路层通信，一个私有 VLAN 域中只有一个隔离 VLAN。
- **团体 VLAN（Community VLAN）**　同一个团体 VLAN 中的端口可以进行数据链路层通信，但不能与其他团体 VLAN 中的端口进行数据链路层通信，一个私有 VLAN 中可以有多个团体 VLAN。

PVLAN 中的端口有如下几种类型。

- **混杂端口（Promiscuous Port）**　混杂端口为主 VLAN 中的端口，可以与任何端口通信，包括同一个 PVLAN 中的隔离端口和团体端口。
- **隔离端口（Isolated Port）**　隔离端口为隔离 VLAN 中的端口，隔离端口只能与混杂端口进行通信。
- **团体端口（Community Port）**　团体端口为团体 VLAN 中的端口，同一个团体 VLAN 中的团体端口之间可以相互通信，且团体端口可以与混杂端口通信，但不能与其他团体 VLAN 的端口进行通信。

如图 7-1 所示的网络中，通过 PVLAN 技术针对不同的部门配置不同的 VLAN 类型，从而实现部门间的隔离或部门内部计算机的隔离。

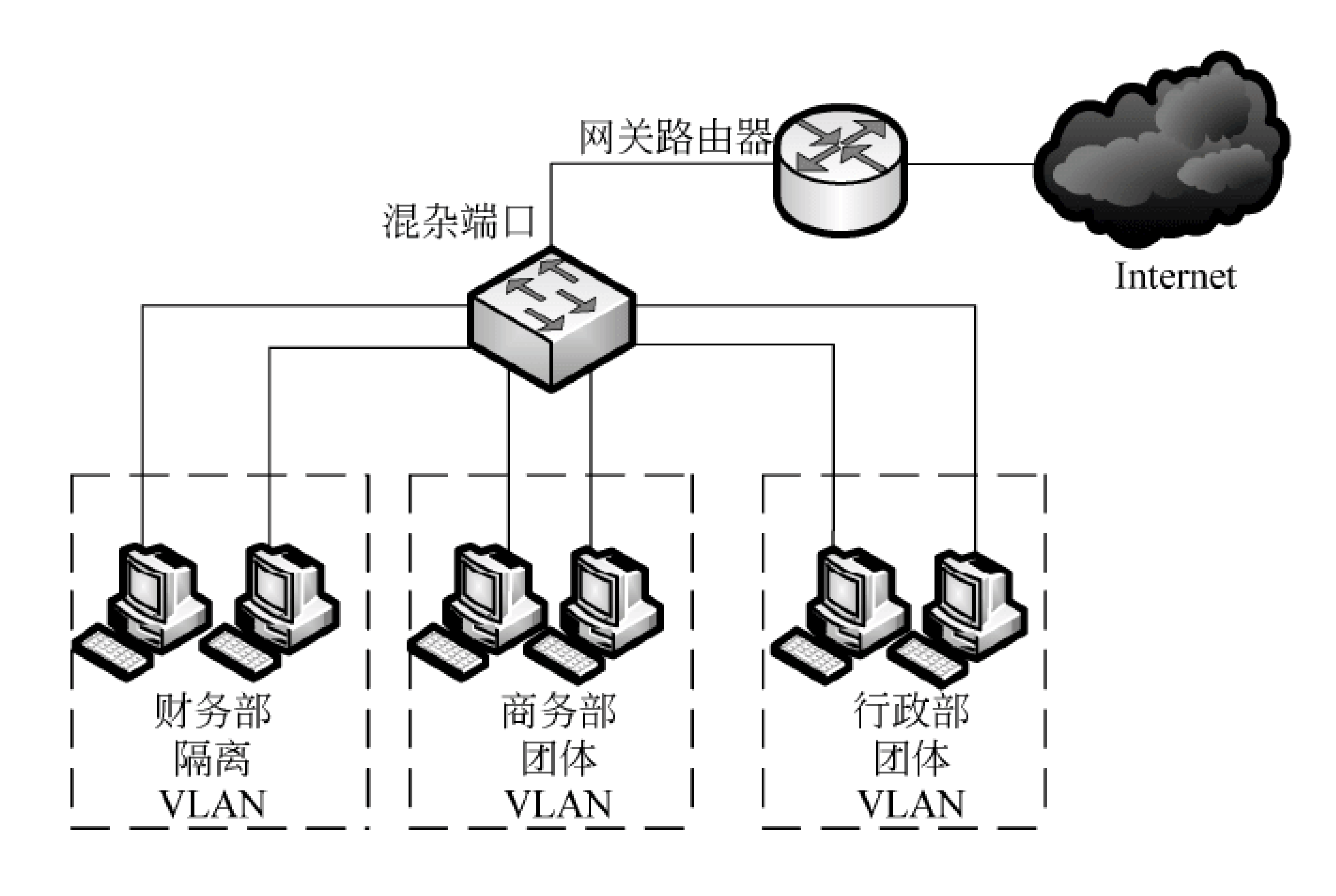


图 7-1　PVLAN 的实现

图 7-1 所示的网络中，主 VLAN 有 3 个部门，其中行政部属于团体 VLAN 10，商务部属于团体 VLAN 20，财务部属于隔离 VLAN 30。由于 3 个部门属于同一个主 VLAN，所以 3 个部门中计算机的 IP 地址都属于同一个子网。行政部及商务部里的各设备能够通信，财务部门的设备属于隔离 VLAN，因此互相之间不能通信。但 3 个部门中各设备都能与主 VLAN 中的混杂端口通信而实现对其他网络的访问。

7.2.2　配置 PVLAN

在交换机上配置 PVLAN，并使其处于 Active（激活）状态，则必须满足以下条件。

- 具有主 VLAN。
- 具有辅助 VLAN。
- 辅助 VLAN 和主 VLAN 进行关联。
- 主 VLAN 内有混杂端口。

1. 配置主 VLAN 与辅助 VLAN

进行主 VLAN 与辅助 VLAN 设置，也即指定 VLAN 类型的过程，其语法格式如下所示。

```
Switch(config-vlan)#private-vlan {community|isolated|primary}
```

2. 关联辅助 VLAN 到主 VLAN

该条件下，首先需要进入主 VLAN 的 VLAN 配置模式，然后再关联辅助 VLAN 到主 VLAN，其语法格式分别如下所示。

```
Switch(config)#vlan primary_vid
Switch(config-vlan)#private-vlan association [add|remove] isolated_vid
```

3. 映射辅助 VLAN 到主 VLAN 的网络接口

该条件下，首先进入主 VLAN 的 VLAN 的端口模式，然后再将辅助 VLAN 映射到主 VLAN 的网络接口，其语法格式分别如下所示。

```
Switch(config)#interface vlan primay_vid
Switch(config-if)#private-vlan mapping [add|move] isolated_vid
```


4. 配置主机端口

配置交换机端口为主机端口时，需要进入连接计算机的端口，把它配置为主机端口，并将其关联到 PVLAN，其语法格式分别如下所示。

```
Switch(config)#interface port-type port
Switch(config)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association primary_vid
isolated_vid
```

5. 配置混杂端口

配置混杂端口时，首先进入主机端口，然后配置其为混杂端口，最后配置混杂端口所在的主 VLAN 及关联的辅助 VLAN，其语法格式分别如下所示。

```
Switch(config)#interface port-type port
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping primary_vid [add|move]
isolated_vid
```

在图 7-2 所示的拓扑图中，设置 VLAN10 为 Primary VLAN，VLAN20 为 Community VLAN，VLAN30 为 Isolated VLAN。端口 F0/1 和 F0/2 为 VLAN30 的端口，端口 F0/3 和端口 F0/4 为 VLAN20 的端口，端口 F0/5 为 Private VLAN 的混杂端口，与 VLAN20 和 VLAN30 关联。

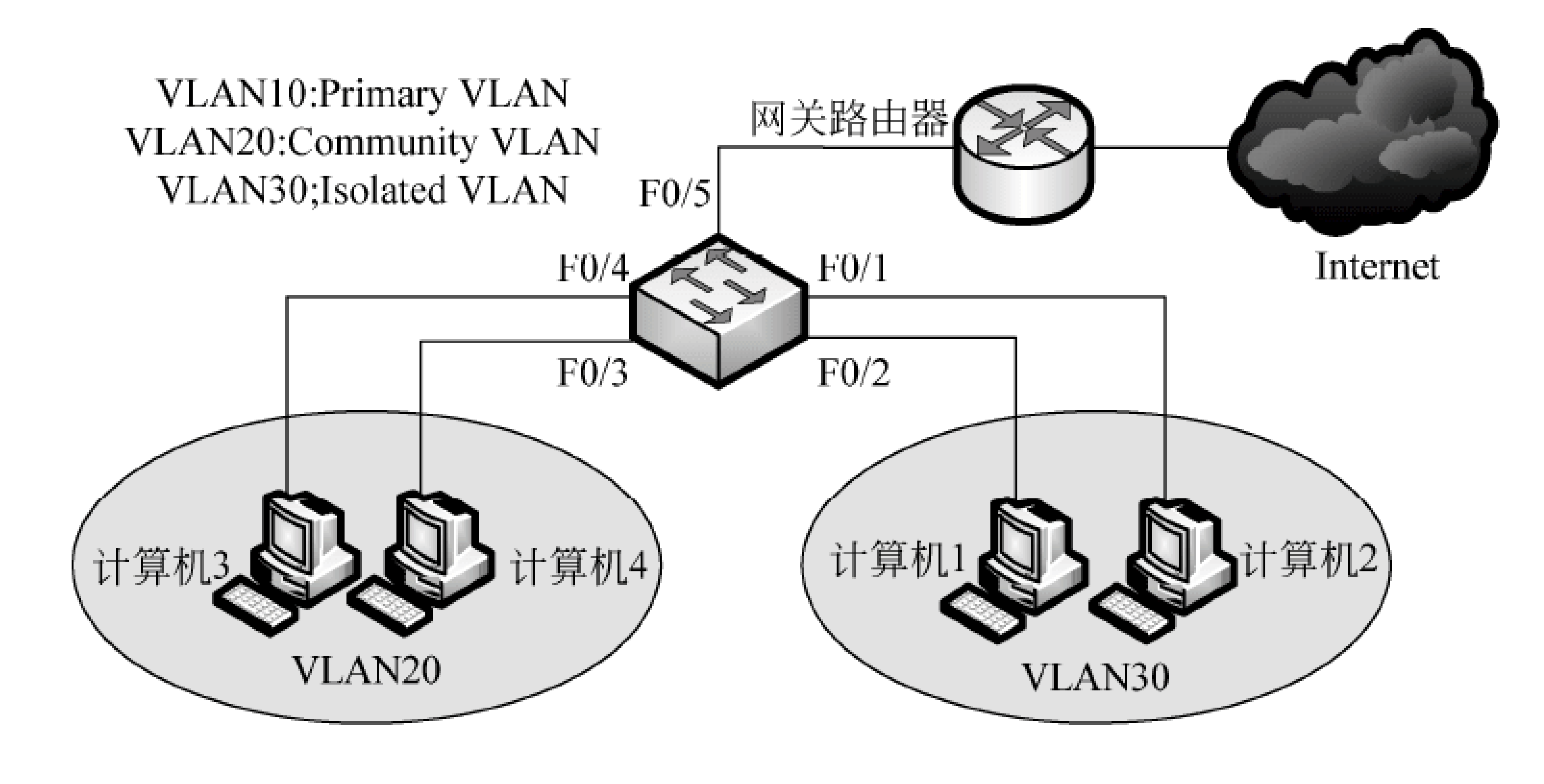


图 7-2　Private VLAN 实例

若要实现图 7-2 实例中的需求，在交换机上可进行如下配置。

```
Switch# configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#private-vlan community
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#private-vlan isolated
Switch(config-vlan)#exit
Switch(config)#vlan 10
Switch(config-vlan)#private-vlan association add 20,30
Switch(config-vlan)#exit
Switch(config)#interface range fastethernet 0/1-2
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 10 30
Switch(config-if-range)#exit
Switch(config)#interface range fastethernet 0/3-4
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 10 20
Switch(config-if-range)#exit
Switch(config)#interface range fastethernet 0/5
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 10 add 20,30
Switch(config-if)#end
Switch# copy running-config startup-config
```

使用如下命令可查看 Private VLAN 的配置及状态信息。

```
Switch#show vlan private-vlan [primary|community|isolated]
```

其中，参数 primary 表示显示主 VLAN 信息；community 表示显示团体 VLAN 信息；isolated 表示显示隔离 VLAN 信息。

7.2.3　网管心得——VLAN 技术白皮书

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

目前，VLAN 技术在交换机上的实现方法，可以大致划分为 4 类。

1. 基于端口 VLAN 技术

利用交换机的端口来划分 VLAN，使被设定的端口都在同一个广播域中，这样划分的 VLAN 也称为静态 VLAN 技术（因为用端口划分 VLAN 将交换机的端口与 VLAN 进行了相应的绑定）。

基于端口的 VLAN 的划分是最简单、有效地 VLAN 划分方法，它按照局域网交换机端口来定义 VLAN 成员。VLAN 从逻辑上把局域网交换机的端口划分开来，从而把终端系统划分为不同的部分，各部分相对独立，在功能上模拟了传统的局域网。

例如，一个交换机的一些端口（1、2）被定义为 VLAN1，同一交换机的另一些端口（3、4）则被定义为 VLAN2。这样做允许各端口之间通信，并允许共享型网络的升级。但是，这种划分模式将虚拟网限制在一台交换机上，如图 7-3 所示。

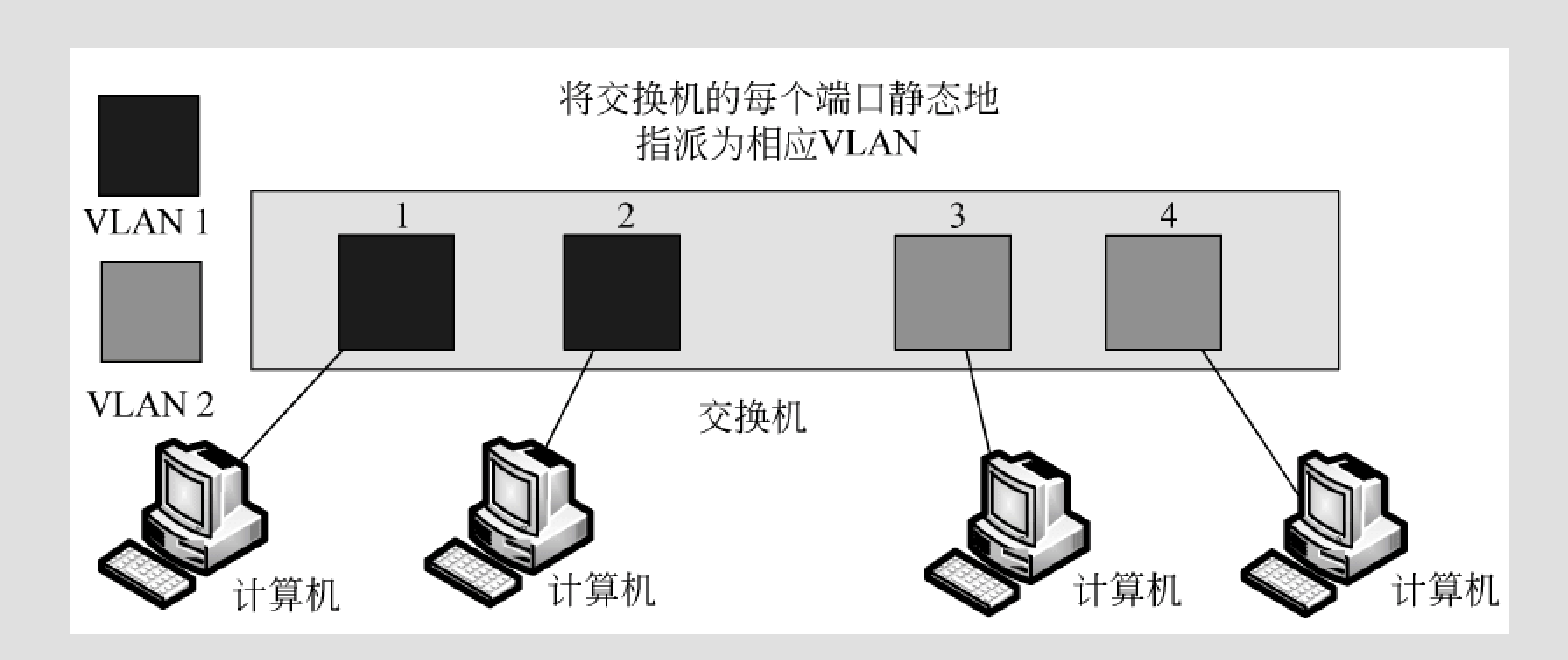


图 7-3　基于端口划分 VLAN 基本结构图

第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN，不同交换机上的若干个端口可以组成同一个虚拟网。

以交换机端口来划分网络成员，其配置过程简单明了。因此，从目前来看，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方法。

2. 基于 MAC 地址 VLAN 技术

根据 MAC 地址所划分的 VLAN，称为动态 VLAN 技术。这种划分 VLAN 的方法是根据每个计算机的 MAC 地址来划分，即对每个 MAC 地址的计算机都配置它属于哪个 VLAN，如图 7-4 所示。

利用这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他交换机时，VLAN 不用重新配置，可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN。这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置非常烦琐。

而且这种划分的方法也导致交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包。

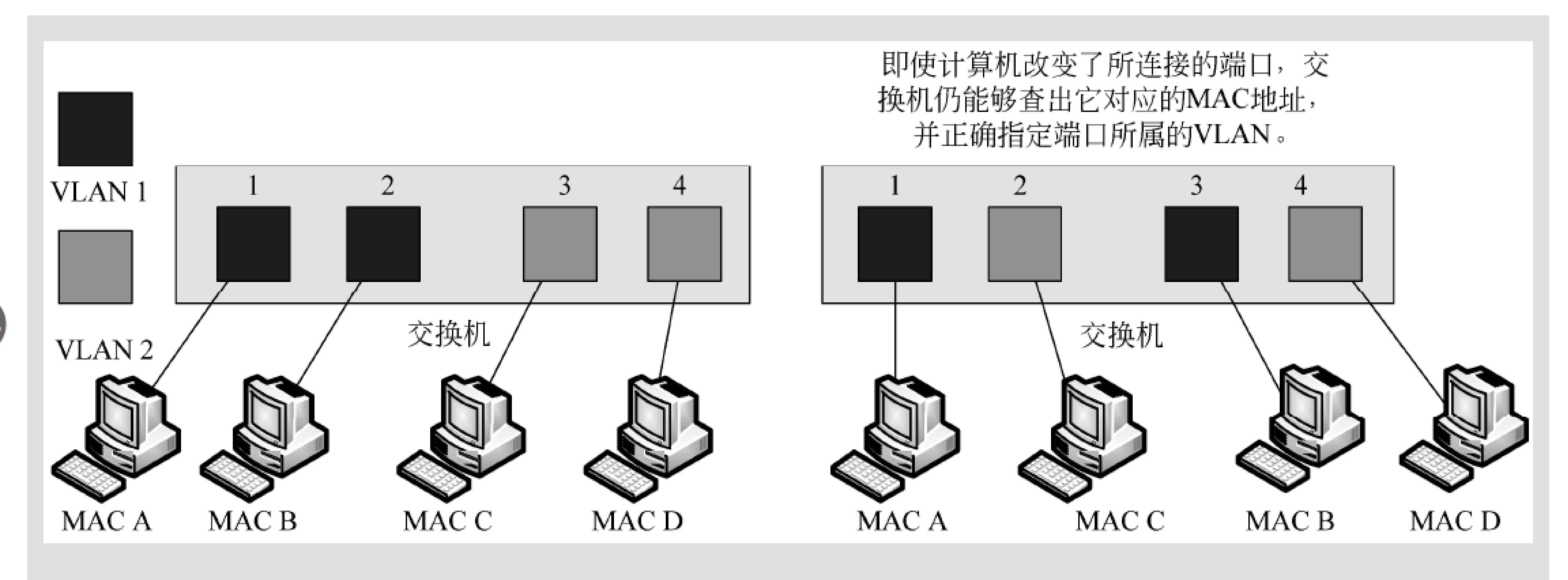


图 7-4　基于 MAC 地址划分 VLAN 结构图

3. 基于 IP 组播 VLAN 技术

组播作为一点对多点的通信，是节省网络带宽的有效方法之一。它能够使一个或多个发送者将数据帧发送给一个组地址，而不是单台计算机。一个 VLAN 就是一个逻辑的组播域，即 IP 组播实际上也是一种 VLAN 的定义，如图 7-5 所示。

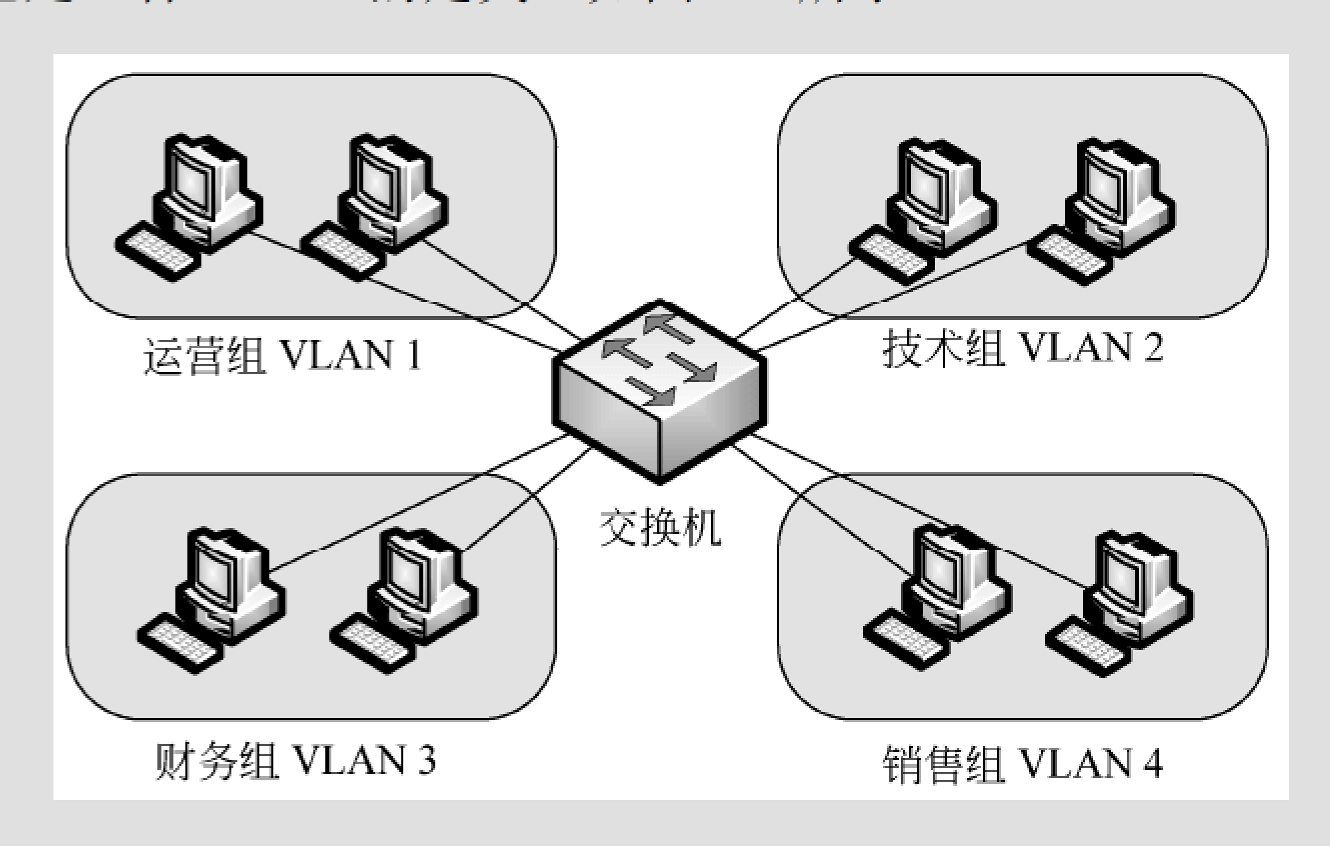


图 7-5　基于 IP 组播划分 VLAN 结构图

基于组播的 VLAN 技术，是动态地把那些需要同时通信的端口定义到一个 VLAN 中，并在 VLAN 中用广播的方法解决点对多点通信的问题，扩大了广域网。从实际意义上来讲，具有更大的灵活性，而且也很容易通过路由器进行扩展，但这种方法不适合局域网（效率不高）。

4. 基于策略 VLAN 技术

基于策略 VLAN 技术也称为基于规则的 VLAN 技术。这是最灵活的 VLAN 划分方法，具有自动配置的能力，能够把相关的用户连在一起。网络管理员只需在网管软件中规定好划分 VLAN 的规则（或属性），那么当一个站点加入到网络中时，将会遵循该规则，并被自动地加入到正确的 VLAN 中。同时对站点的移动和改变也可进行自动的调整。

使用这种划分 VLAN 的方法，整个网络可以非常方便地通过路由器扩展网络的规模。有的产品还支持一个端口分别加入到不同的 VLAN 中，这在交换机与共享式 HUB（集线器）共

存的环境中显得很重要。自动配置 VLAN 时，交换机中软件自动检查进入交换机端口的广播信息的 IP 源地址，然后软件自动将这个端口分配给一个由 IP 子网映射的其他 VLAN。

5. 按用户要求 VLAN 技术

基于用户定义划分 VLAN 是指根据具体的网络用户的特别要求来定义和设计 VLAN，而且可以让非 VLAN 群体用户访问该 VLAN，但是需要提供用户名和密码，在得到 VLAN 管理的认证后才可加入 VLAN 中。

综合所述，基于端口的 VLAN 端口划分方式建立在物理层上；MAC 地址划分 VLAN 端口方式建立在数据链路层；网络层和 IP 组播方式则建立在网络层上。其中最常用到的划分方式有基于端口（静态 VLAN）和 MAC 地址（动态 VLAN）这两种。

7.3 基于端口的认证安全

基于端口的网络接入控制（Port Based Network Access Control）是指在局域网接入设备的端口，对所接入的设备进行认证和控制。如果连接到端口上的设备能够通过认证，则端口就被开放，终端设备就被允许访问局域网中的资源；相反，则端口就相当于被关闭，终端设备将无法访问局域网中的资源。802.1x 协议就是一种基于端口的网络接入的协议。

7.3.1 IEEE 802.1x 认证介绍

IEEE 802.1x 协议是基于客户端/服务器的访问控制和认证协议，它可以限制未经授权的用户/设备通过接入端口（Access Port）访问局域网或广域网。在获得交换机或局域网提供的各种业务之前，802.1x 对连接到交换机端口上的用户/设备进行认证，且在认证通过之前，802.1x 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过之后，正常的数据才可以顺利地通过以太网端口。

在访问控制流程中，网络访问技术的核心部分端口访问实体（PAE）包含认证者（对接入的用户/设备进行认证的端口）、请求者（被认证的用户/设备）和认证服务器（根据认证者的信息，对请求访问网络资源的用户/设备进行实际认证功能的设备）3 个部分。

以太网的每个物理端口被分为受控和不受控的两个逻辑端口，物理端口收到的每个帧都被送到受控和不受控端口。其中，不受控端口始终处于双向连通状态，主要用于传输认证信息。而受控端口的连通或断开是由该端口的授权状态决定的。认证者的 PAE 根据认证服务器认证过程的结果，控制“受控端口”的授权或未授权状态。处在未授权状态的控制端口将拒绝用户或设备的访问。受控端口与不受控端口的划分，分离了认证数据和业务数据，提高了系统的接入管理和接入服务的工作效率。

1. IEEE 802.1x 认证特点

基于以太网端口认证的 802.1x 协议的特点包括的 IEEE 802.1x 协议为二层协议，不需要到达三层，对设备的整体性能要求不高，可以有效降低构建网络的成本；借用了在 RAS（Remote

Access Service，远程访问服务）系统中常用的 EAP（扩展认证协议），可以提供良好的扩展性和适应性，实现对传统 PPP 认证架构的兼容；802.1x 的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而实现业务与认证的分离，由 RADIUS 认证服务器和交换机利用不可控的逻辑端口共同完成对用户的认证与控制，业务报文直接承载在正常的二层报文上通过可控端口进行交换，通过认证之后的数据包是无需封装的纯数据包；可以使用现有的后台认证系统降低部署的成本，并有丰富的业务支持；可以映射不同的用户认证等级到不同的 VLAN；可以使交换端口和无线局域网具有安全的认证接入功能。

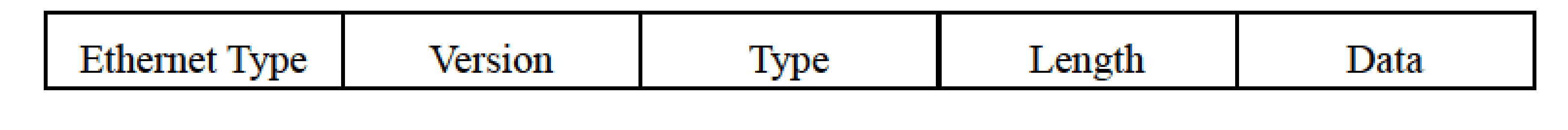
2. IEEE 802.1x 工作过程

因 IEEE 802.1x 协议是基于客户端/服务器的访问控制和认证协议，所以其工作过程也就是客户端提供认证信息并由服务器进行认证的过程。具体可分为以下步骤。

- 当用户有上网需求时，打开 802.1x 客户端程序，并输入已经申请、登记过的用户名和口令，发起连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。
- 交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名传送给自己。
- 客户端程序响应交换机发出的请求，将用户名信息通过数据帧送给交换机。交换机将客户端传来的数据帧，经过封包处理后送给认证服务器进行处理。
- 认证服务器收到交换机转发的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字段对它进行加密处理，同时也将此加密字传送给交换机，由交换机传给客户端程序。
- 客户端程序收到由交换机传来的加密字段后，用该加密字段对口令部分进行加密处理（此种加密算法通常是不可逆的），并通过交换机传给认证服务器。
- 认证服务器将传送来的加密后的口令信息和其经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向交换机发出打开端口的指令，允许用户的业务流通过端口访问网络。否则，反馈认证失败的消息，并保持交换机端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过。

3. IEEE 802.1x 数据包格式

EAPoL 是 IEEE 802.1x 标准定义的一种报文封装格式，如图 7-6 所示，主要用于客户端和交换机之间，它使交互的 EAP 协议报文能够在局域网协议上传输。



Ethernet Type	Version	Type	Length	Data

图 7-6　EAPoL 报文格式

- Ethernet Type，以太网帧头中的以太网类型。对于 IEEE 802.1x 报文，协议类型为 0x888E。
- Version 发送方支持的协议版本号。
- Type 表示 802.1x 报文的类型。00 为 EAP-Packet，表示认证信息帧，用于承载认证信

息；01 为 Start，即 EAP-Start，表示发起 802.1x 认证；02 为 EAP-Logoff，表示退出认证；03 为 EAP-Key，表示密钥信息帧；04 为 Encapsulated ASP Alert，用于支持 ASF（Alerting Standards Forum）的 Alerting 信息。

- ❑ Length 表示 Date 字段的长度。如果为 0，代表 Date 字段不存在任何数据。
- ❑ Date 根据不同的 Type 有不同的格式。

当 EAPoL 数据包中的 Type 字段为 EAP-Packet（00）时，EAPoL 中的 Date 字段为 EAP 数据包，格式如图 7-7 所示。

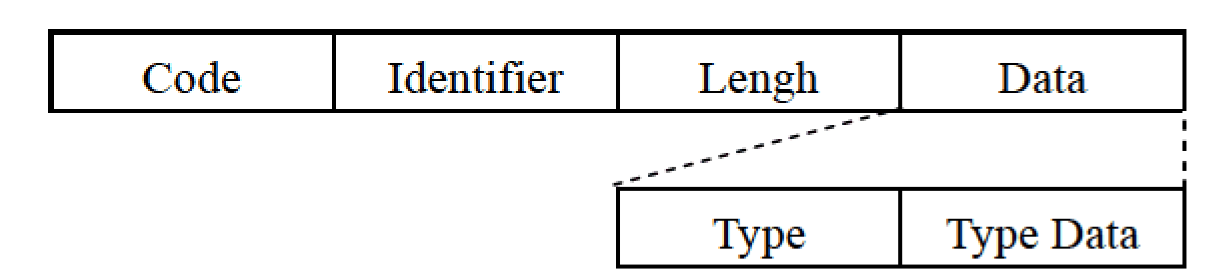


图 7-7　EAP 报文格式

- ❑ Code 表示 EAP 报文的类型，包括 Request、Response、Success、Failure。
- ❑ Identifier 进行 Request 与 Response 消息的匹配。
- ❑ Length EAP 报文的长度，包括 Code、Identifier、Length、Date。
- ❑ Date 由 Code 字段决定。Success 与 Failure 类型的报文不存在 Date 字段；Request 与 Response 类型的报文存在 Date 字段，且 Date 字段中包括 Type 与 Type Date 字段。
- ❑ Type 表示 EAP 的认证类型。1 代表 Identity，用于查询身份；4 代表 MD5 Challenge，包含挑战信息。
- ❑ Type Date 根据不同 Type 的 Request 和 Response 而定。

4. IEEE 802.1x 定时器

802.1x 认证使用了多个定时器，以保证认证过程的正常进行以及认证组件间的故障检测等。

❑ **安静定时器（quiet-period）**

当客户端认证失败后，交换机需要等待一段时间（默认为 60 秒）才会再处理客户端的认证请求，这段时间即为 quiet-period。此定时器主要用于防止用户频繁地对交换机发送认证请求而对交换机造成的威胁。

❑ **重新认证定时器（re-authperiod）**

用户通过认证后，交换机可以主动请求客户端进行重认证。re-authperiod 表示请求客户端重认证的时间间隔（默认为 30 秒）。重认证机制主要用于检测用户是否还在线，使计费更加正确，而且可以防止非法用户的冒用。

❑ **服务器超时定时器（server-timeout）**

认证服务器（RADIUS）的最大响应时间（默认为 60 秒）。如果在该时间间隔内，服务器没有对交换机发送的认证请求进行响应，交换机重发认证请求。

❑ **客户端超时定时器（supp-timeout）**

该计时器表示当交换机向客户端发送 EAP-Request 或 MD5 Challenge 报文请求 MD5 散列值后，等待客户端响应的时间（默认为 30 秒）。

❑ 发送超时定时器（tx-period）

当客户端发起认证过程后，交换机需向客户发送 EAP-Request 或 Identity 请求客户端发送用户名信息，此时交换机启动 tx-period 定时器（默认为 5 秒）。若该定时器超时前客户端没有响应 EAP-Request 或 Identity 报文，交换机将重发请求报文。

5．IEEE 802.1x 的应用环境

综合 IEEE 802.1x 的特点和工作过程分析，它较为适应的网络环境有以下两种。

❑ 交换式以太网络环境

对于交换式以太网络中，用户和网络之间采用点到点的物理连接，用户彼此之间通过 VLAN 隔离，此网络环境下，网络管理控制的关键是用户接入控制，802.1x 不需要提供过多的安全机制。

❑ 共享式网络环境

当 802.1x 应用于共享式的网络环境时，为了防止在共享式的网络环境中出现类似“搭载”的问题，有必要将 PAE 实体由物理端口进一步扩展为多个互相独立的逻辑端口。逻辑端口和用户或设备形成一一对应关系，并且各逻辑端口之间的认证过程和结果相互独立。在共享式网络中，用户之间共享接入物理媒介，接入网络的管理控制必须兼顾用户接入控制和用户数据安全，可以采用的安全措施是对 EAPoL 和用户的其他数据进行加密封装。在实际网络环境中，可以通过加速 WEP 密钥重分配周期，弥补 WEP（Wired Equivalent Privacy 加密技术，源自于 RSA 数据加密技术，以满足用户更高层次的网络安全需求）静态分配秘钥导致的安全性的缺陷。

6．IEEE 802.1x 的安全性分析

802.1x 协议中，有关安全性的问题一直是 802.1x 反对者攻击的重点，但通过 802.1x 与 EAP 的结合使用，可以提供灵活、多样的认证解决方案。综合 IEEE 802.1x 的技术特点，它具有的优势可概括为以下几点。

❑ 简洁高效

纯以太网技术内核，保持了 IP 网络无连接特性，不需要进行协议间的多层封装，去除了不必要的开销和冗余；消除网络认证计费瓶颈和单点故障，易于支持多业务和新兴流媒体业务。

❑ 容易实现

可在普通 L3、L2、IPDSLAM 上实现，网络综合造价成本低，保留了传统 AAA 认证的网络架构，可以利用现有的 RADIUS 设备。

❑ 安全可靠

在二层网络上实现用户认证，结合 MAC、端口、账户、VLAN 和密码等；绑定技术具有很高的安全性，在无线局域网网络环境中 802.1x 结合 EAP－TLS，EAP－TTLS，可以实现对 WEP 证书密钥的动态分配，克服无线局域网接入中的安全漏洞。

❑ 应用灵活

可以灵活控制认证的精确度，用于对单个用户连接、用户 ID 或者是对接入设备进行认证，认证的层次可以进行灵活的组合，满足特定的接入技术或者是业务的需要。

❑ 易于运营

控制流和业务流完全分离，易于实现跨平台多业务运营，少量改造传统包月制等单一收费制网络即可升级成运营级网络，而且网络的运营成本也有望降低。

IEEE 802.1x 协议具有完备的用户认证、管理功能，可以很好地支撑宽带网络的计费、安全、运营和管理要求，对宽带 IP 城域网等电信级网络的运营和管理具有极大的优势。IEEE 802.1x 协议对认证方式和认证体系结构上进行了优化，解决了传统 PPPOE（一种局域网连接方式）和 Web/PORTAL 认证方式带来的问题，更加适合在宽带以太网中的使用。

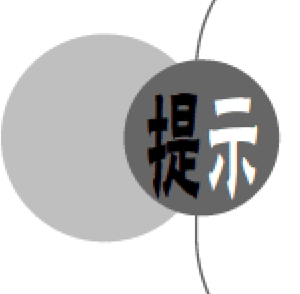
7.3.2 配置 IEEE 802.1x 认证

根据 IEEE 802.1x 认证的原理和工作过程的需要，在对其进行配置时可分为 AAA 与 RADIUS 配置和启用 IEEE 802.1x 认证两个阶段。

1. AAA 与 RADIUS 配置

在交换机上，由于 IEEE 802.1x 的实现是基于 AAA（Authentication、Authorization、Accounting，认证、授权、计费）的，所以在启用 IEEE 802.1x 认证之前需先启用 AAA 功能。其语法格式如下所示。

```
Switch(config)#aaa new-model
```



AAA 是一个提供网络访问控制安全的模型，通常用于用户登录设备或接入网络。AAA 以模块方式提供了对认证、授权和计费功能的一致性框架，Authentication 认证模块可验证用户是否可获得访问权；Authorization 授权模块能够定义用户可使用哪些服务或权限；Accounting 计费模块可记录用户使用网络资源的情况。

交换机上需要将 IEEE 802.1x 认证请求发送到特定的 RADIUS 认证服务器来进行身份验证，但在配置交换机与 RADIUS 认证服务器通信之前，需要为 RADIUS 认证服务器配置一个 IP 地址，其语法格式如下所示。

```
Switch(config)#radius-server host ip-address [auth-port number | acct-port
number]
```

❑ auth-port 代表配置 RADIUS 认证服务器的认证和授权端口号。默认情况下，其端口号为 UDP 1812。

❑ acct-port 代表配置 RADIUS 认证服务器的计费端口号。默认情况下，其端口号为 UDP 1813。



一些较老的 RADIUS 认证服务器实现是使用 UDP 1645 和 1646 作为认证授权和计费端口，需要根据实际情况配置正确的端口号。

还可以使用此命令添加多个 RADIUS 认证服务器，当一个 RADIUS 认证服务器不可用时，交换机将按照配置的顺序进行查找，来使用下一个配置的 RADIUS 认证服务器。

另外，认证过程中若要使交换机与 RADIUS 认证服务器之间能够正常工作，还需配置 RADIUS 服务器认证密钥，用来提供交换机与 RADIUS 认证服务器之间通信的安全性。其语法格式如下所示。

```
Switch(config)#radius-server host key {0 string | 7 string | string}
```

该命令中设置的密钥必须与 RADIUS 认证服务器中设置的密钥相匹配，否则 RADIUS 服务器将丢弃认证报文。

然后，需要在交换机上配置 IEEE 802.1x 的认证列表，列表中包括使用的认证方式，如使用 RADIUS 服务器或本地认证等。其语法格式为：

```
Switch(config)#aaa authentication dot1x {default | list-name} method1
[method2...]
```

- default 代表定义默认的认证列表。当没有指定 IEEE 802.1x 引用的特定验证列表时，交换机将使用默认列表中定义的参数进行验证。
- list-name 代表创建并命名一个新的验证列表。
- method 代表验证使用的方法。

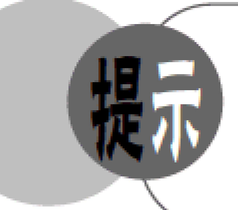
验证方法可使用 group radius，即使用 RADIUS 服务器进行验证；group group-name 表示使用 RADIUS 服务器组中的服务器进行验证；local 表示使用本地数据库中的用户名和密码进行验证；none 表示无需进行验证，用户即可通过。此外，一个验证列表中可指定多个验证方式。需要注意的是，当指定为 none 后，将无法再指定其他验证方式，none 通常用于网络或服务不可用时的最后解决方案。

2. 启用 IEEE 802.1x

进行 RADIUS 服务器的相关配置后，即完成了 IEEE 802.1x 的准备配置工作。这时，就可以在交换机的特定端口启用 IEEE 802.1x 功能，其语法格式如下所示。

```
Switch(config-if)#dot1x port-control auto
```

当对端口配置此命令后，端口将只接收 EAPoL 报文，并且只有认证通过后，端口才会接收其他报文，如用户数据报文。



在某些较老版本的交换机上，启用 IEEE 802.1x 需要在全局配置模式下执行 aaa authentication dotlx 命令，且不支持配置验证列表。

启用 IEEE 802.1x 功能后，默认情况下交换机将使用默认的验证列表（default）进行验证。但还可以在全局配置模式下，更改 IEEE 802.1x 认证所使用的验证列表。其语法格式为：

```
Switch(config)#dot1x authentication {default | list-name}
```

- default 代表使用默认的验证列表。

- list-name 代表使用自定义的验证列表，此处指定的验证列表名称必须与之前使用 aaa authentication dotlx list-name 命令定义的名称相同。

例如，在思科交换机上，配置 AAA 及 RADIUS 服务器（IP 地址为 10.1.1.1、密钥为 12345、认证列表名称为 slkj，并采用 RADIUS 服务器认证方式），然后在 fastethernet 0/1 和 fastethernet 0/2 端口启用 IEEE 802.1x 认证，可进行如下配置。

```
Switch#configure terminal
Enter configiration commands, one per line. End with CNTL/Z.
Switch(config)#aaa new-model
Switch(config)#radius-server host 10.1.1.1
Switch(config)#radius-server key 12345
Switch(config)#aaa authentication dot1x slkj group radius
Switch(config)#dotlx authentication slkj
Switch(config)#interface fastethernet 0/1
Switch(config-if)#dotlx port-control auto
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/2
Switch(config-if)#dotlx port-control auto
Switch(config-if)#exit
Switch# copy running-config startup-config
```

7.3.3 配置重新认证周期

在交换机上配置 IEEE 802.1x 过程中，可以通过命令开启并配置设备对 IEEE 802.1x 用户主动发起的周期性重认证功能，其取值范围为 1～65535。

端口启动了 802.1x 的周期性重认证功能后，设备会根据周期性重认证定时器设定的时间间隔，定期启动对该端口在线 802.1x 用户的认证，以检测用户连接状态的变化，更新服务器下发的授权属性（例如 ACL、VLAN、QoS Profile），确保用户的正常在线。

在思科交换机上，对重新认证周期功能开启和配置，其语法格式分别如下所示。

```
Switch(config-if)#dotlx reauthentication
Switch(config-if)#dotlx timeout reauth-period time
```

例如，在交换机的 fastethernet1/1 端口开启并设置其重认证周期为 40 秒，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)#dotlx reauthentication
Switch(config-if)# Switch(config-if)#dotlx timeout reauth-period 40
Switch(config-if)#end
Switch# copy running-config startup-config
```

7.3.4　修改安静周期

同样，在配置 IEEE 802.1x 过程中，还可以通过命令来更改设备上特定端口的安静周期，其取值范围为 1～65535 秒。当 802.1x 用户认证失败以后，设备需要静默一段时间，然后再重新发起认证，且在安静周期内，设备不进行 802.1x 认证的相关处理。

在交换机上，进行安静周期的配置，其语法格式如下所示。

```
Switch(config-if)#dotlx timeout quiet-period time
```

例如，将交换机的 fastethernet1/1 端口的安静周期设置为 40 秒，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)# dotlx timeout quiet-period 40
Switch(config-if)#end
Switch# copy running-config startup-config
```

7.4　配置 RMON

RMON 是 IETF（Internet Engineering Task Force，互联网工程任务组）标准的监控规范，该规范能够以网络管理者身份交换对网络的监控数据。用户可以配置并使用交换机上的 RMON 功能，来监控所有相连网络中交换机间数据流的流动情况，从而更好地保护设备及网络的安全。

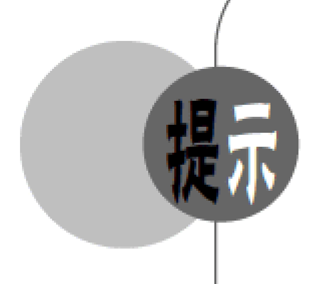
7.4.1　默认的 RMON 配置

RMON（Remote Network Monitoring）远端网络监控，最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题。RMON 规范是由SNMP（Simple Network Management Protocol，简单网络管理协议）中的MIB扩展而来。RMON 中，网络监视数据包含了一组统计数据和性能指标，它们在不同的监视器（或称探测器）和控制台系统之间相互交换。结果数据可用来监控网络利用率，以用于网络规划，性能优化和协助网络错误诊断。

当前 RMON 有 RMON v1 和 RMON v2 两种版本。RMON v1 在目前使用较为广泛的网络硬件中都能发现，它定义了 9 个 MIB 组服务于基本网络监控；RMON v2 是 RMON v1 的扩展，专注于 MAC 层以上的流量层，它主要强调 IP 流量和应用程序层流量。RMON v2 允许网络管理应用程序监控所有网络层的信息包，这与 RMON v1 不同，后者只允许监控 MAC 及其以下层的信息包。

RMON 监视系统由探测器（代理或监视器）和管理站两部分构成。RMON 代理在 RMON MIB 中存储网络信息，它们被直接植入网络设备（如路由器、交换机等），也可以是计算机上运行的一个程序。代理只能看到流经它们的流量，所以在每个被监控的 LAN 段或 WAN 链接

点都要设置 RMON 代理，网管工作站用 SNMP 获取 RMON 数据信息。



MIB（Management Information Base，管理信息库），它是网络管理数据的标准，在这个标准中规定了网络代理设备必须保存的数据项目、数据类型及允许在每个数据项目中的操作。通过对这些数据项目的存取访问，可以得到该网关的所有统计内容，然后通过对多个网关统计内容的综合分析即可实现基本的网络管理。

默认情况下，交换机支持 RMON 中的第 1、2、3、9 组（统计组、历史组、警报组、事件组）的内容，且所有 RMON 功能均被关闭。

❑ **统计组**

统计组（Statistics）是 RMON 中的第 1 组，用于统计被监控的每个子网的基本统计信息。目前只能对网络设备的以太网接口进行监控、统计。

❑ **历史组**

历史组（History）是 RMON 中的第 2 组，它定期地收集统计网络值的记录并为日后的处理把统计存储起来，又包含 HistoryControl 和 EthernetHistory 两个小组，HistoryControl 组用来设置采样间隔时间等控制信息；EthernetHistory 组为管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

❑ **警报组**

警报组（Alarm）是 RMON 中的第 3 组，以指定的时间间隔监控一个特定的 MIB 对象，当这个 MIB 对象的值超过一个设定的上限值或低于一个设定的下限值时，会触发一个警报。警报被当作事件来处理，处理事件的方式可以是记录日志或发送 SNMP Trap 的方式。

❑ **事件组**

事件组（Event）是 RMON 中的第 9 组，决定当由于警报而产生事件时，处理行为将产生一个日志记录表项或者一个 SNMP Trap。

7.4.2 配置 RMON 警报和事件

用户可以通过命令行或一个 SNMP 网络管理工作站来配置 RMON，不过建议用户最好使用 NMS（网络管理工作站）上的一般的 RMON 管理工具来实现 RMON 的管理，以便充分利用 RMON 的网络管理功能。

在交换机上，配置 RMON 的报警和事件功能，可依次分为设置针对一个 MIB 对象的警报功能，和当警报产生时，增加相应的事件表项并作相应的处理两个步骤。

1. 配置 RMON 警报

若要在交换机上，针对一个 MIB 对象设置 RMON 警报功能，其语法格式分别如下所示。

```
Switch(config)#rmon alarm number variable interval {delta | absolute} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]
```

- number 指定这个警报表项的索引（编号），其取值范围为 1~65535。
- variable 代表要控制 MIB 的变量标识符，这个变量必须是整型类数据类型。
- interval 指定采样的时间间隔（单位为秒），取值范围为 1~2147483647 秒。关键字 date 表示取样的值，是指 MIB 变量在两次取样间值的变化；而关键字 absolute 表示直接使用 MIB 变量的值作为取样值。
- value 指定警报触发的条件。即当 MIB 变量的值变化为大于关键字 rising-threshold 后面指定的 value 值（从小于这个值变为大于这个值）或变为小于关键字 falling-threshold 后面指定的 value 值时。value 后所跟值的范围是–2147483648~2147483648。



除了首次达到触发条件外，只有同时跨越上限和下限时才会触发，例如从达到或超过上限值的位置，变化为达到或低于下限值位置，以防止不停地触发。

- event-number 代表警报引发的事件产生时，指定事件组产生事件表项的索引，若不指定则不会产生相应的事件（可选）。这个值的取值范围为 1~65535。
- string 标识这个警报表项的拥有者（可选）。

2. 配置 RMON 事件

在交换机上配置 RMON 事件，即当警报产生时，增加相应的事件表项并对这些警报作相应的处理，其语法格式如下所示。

```
Switch(config)#rmon event number [log] [trap community] [description string]
[owner string]
```

- **number**　number 代表这个事件表项的索引，必须和配置 RMON 警报时设置的 event-number 索引匹配。一个警报产生时，若警报指定的 event-number 对应的事件表项不存在（number 不等于 event-number），则不会产生对应的事件。这个值的范围为 1~65535。
- **log**　输入这个关键值，则警报产生时，会将这个事件记录到日志中（可选）。
- **trap**　输入这个关键值，则警报产生时，会产生一个 SNMP Trap（可选）。
- **community**　发送 Trap 时使用的认证名（可选）。
- **description string**　对这个事件的描述（可选）。
- **owner string**　标志这个事件的拥有者（可选）。

用户可以配置对任何一个可统计的 MIB 变量的报警功能。例如，对 MIB-II 中 IfEntry 表中实例 ifInNUcastPkts.6（端口 6 上收到的非单播帧的个数，实例的标识符为 1.3.6.1.2.1.2.2.1.12.6）设置报警功能。

具体实现功能是，交换机每隔 30 秒检查端口 6 上收到的非单播帧个数的变化，如果收到的非单播帧个数比上次检查时（30 秒前）增加了 20 个或 20 个以上，或者比上次只增加 10 个或 10 个以下，则警报被触发；同时警报将触发事件 1 进行相应的操作（记录到日志中，并发送认证名为“rmon”的 Trap、事件的描述为“ifInNUcastPkts is too much”）；警报和事件表项的拥有者均为“slkj”。可进行如下配置。

```
Switch# configure terminal
Switch(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold
20 1 falling-threshold 10 1 owner slkj
Switch(config)#rmon event 1 log trap rmon description "ifInNUcastPkts is too
much" owner slkj
Switch(config)#exit
Switch# copy running-config startup-config
```

另外，在交换机的全局配置模式下，可以输入 no rmon alarm number 命令，并按回车键删除一个警报表项，同样可输入 no rmon event number 命令，然后按回车键来删除一个事件处理表项。

7.4.3 创建历史组表项

用户可针对交换机的端口创建历史组表项（只适用于物理端口），定期地收集统计网络值的记录并为日后的处理把统计存储起来。

在交换机的物理端口，创建历史组表项，其语法格式如下所示。

```
Switch(config-if)#rmon collection history index [owner onwername] [buckets
bucket-number] [interval seconds]
```

- **index** 指定这个历史记录配置表项的索引（编号），其取值范围为 1~65535。
- **owner ownername** 标志这个表项的拥有者（可选）。
- **bucket-number** 每次采样的数据将被保存下来，bucket-number 的值指定了保存每次采样数据的历史记录的最大表项个数。如果历史记录已满，则新的采样数据将覆盖最老的一次采样数据记录。这个值的范围是 1~65535，默认值为 10。
- **interval** 指定采样的时间间隔（单位为秒），其取值范围为 1~3600，默认为 1800 秒。

例如，在交换机的 fastethernet1/1 端口，创建历史组表项，设置其索引值为 40、拥有者名称为 slkj、采样数据的历史记录最大表项个数为 20、采样的时间间隔为 1000 秒，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)# rmon collection history 30 owner slkj buckets 20 interval
1000
Switch(config-if)#end
Switch# copy running-config startup-config
```

另外，还可以通过在交换机的端口模式下，输入 no rmon collection history index 命令，并按回车键来删除一个特定的历史组表项。

7.4.4 创建 RMON 统计组表项

用户还可以针对设备的物理端口创建 RMON 统计表项。当设置了一个端口的统计表项后，

交换机将从这时开始各种数据的统计。

在交换机的物理端口上，创建 RMON 统计表项，其语法格式为：

```
Switch(config-if)#rmon collection stats index [owner ownername]
```

- index 用于指定这个统计表项的索引（编号），取值范围是 1~65535。
- owner ownername 标志这个表项的拥有者（可选）。

例如，在交换机的 fastethernet1/1 端口，创建 RMON 统计表项，设置其索引值为 30，拥有者名称为 slkj，可进行如下配置。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if)# rmon collection stats 30 owner slkj
Switch(config-if)#end
Switch# copy running-config startup-config
```

同样，可以通过在端口配置模式下，输入 no rmon collection stats index 命令，并按回车键来删除一个特定的统计表项。

7.4.5 显示 RMON 的状态

执行配置 RMON 警报和事件、创建历史组表项及创建 RMON 统计组表项操作后，可在交换机的特权模式下，通过使用下列的命令来显示对交换机的各种访问方式的状态。

```
Switch#show rmon alarms
Switch#show rmon events
Switch#show rmon history
Switch#show rmon statistics
```

- show rmon alarms 显示 RMON 警报表的配置信息。
- show rmon events 显示 RMON 事件表的配置信息和查看日志信息。
- show rmon history 显示 RMON 历史表的配置信息和显示采样的历史数据。
- show rmon statistics 显示 RMON 的统计信息。

例如，在交换机上利用 show rmon statistics 命令显示 RMON 的统计表信息。其操作及输出显示如下。

```
Switch#show rmon statistics
Statistics:1
Data source:Fa0/1
DropEvents:0
Octets:1884085
Pkts:3096
BroadcastPkts:161
MulticastPkts:97
CRCAlignErrors:0
```

```
UndersizePkts:0
OversizePkts:0
OversizePkts:1200
Fragments : 0
Jabbers : 0
Collisions : 0
Pkts64Octets : 128
Pkts65to127Octets : 336
Pkts128to255Octets : 229
Pkts256to511Octets : 3
Pkts512to1023Octets : 0
Pkts1024to1518Octets : 1200
Owner : slkj
```

7.5 操作实例

7.5.1 操作实例——破解交换机密码

众所周知交换机和路由器都需要有安全保证，及时配置合理的密码，不仅可以防止网络暴力破解密码，还可以使其得到安全保障。

1. 实例目的

- ❑ 破解密码。
- ❑ 重设密码。

2. 实例步骤

（1）将一台计算机的 COM1 和 2950 交换机的“console”口相连接，图 7-8 为结构拓扑图。

（2）执行【开始】|【程序】|【附件】|【通讯】|【超级终端】命令，在弹出的对话框的【名称】文本框内输入名称，在【图标】列表内选择一个图标。然后，单击【确定】按钮，如图 7-9 所示。

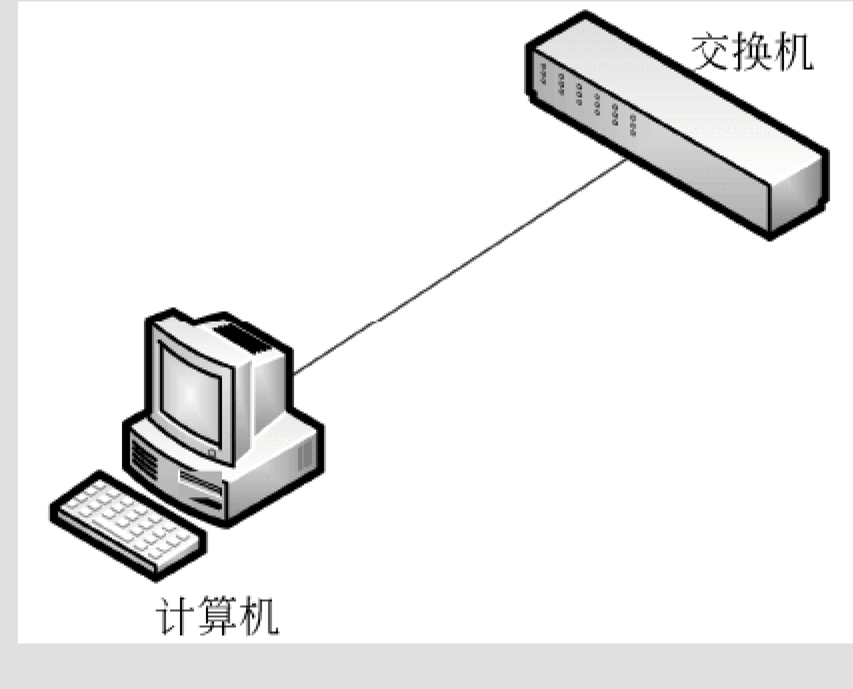


图 7-8 拓扑图



图 7-9 输入名称并选择图标

（3）在【连接到】对话框中，单击【连接时使用】下拉按钮，选择 COM1 选项，如图 7-10 所示。

（4）在弹出的对话框中，单击【还原为默认值】按钮，然后依次单击【应用】和【确定】按钮，如图 7-11 所示。

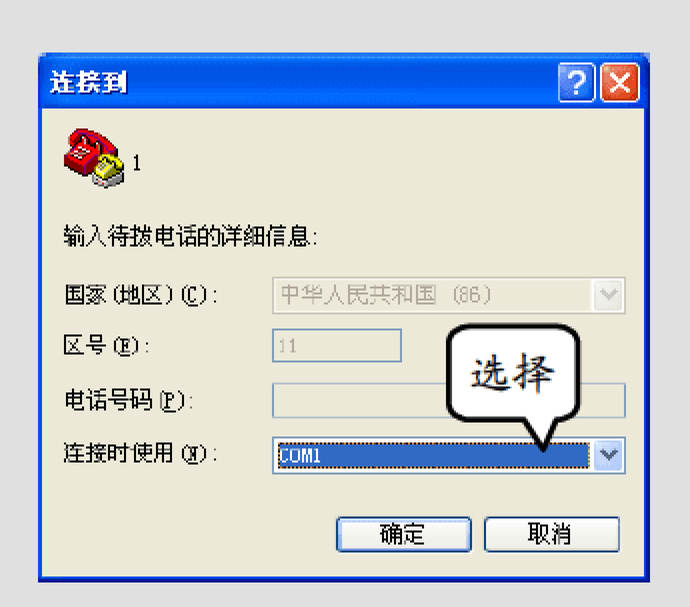


图 7-10　选择 COM1 口配置

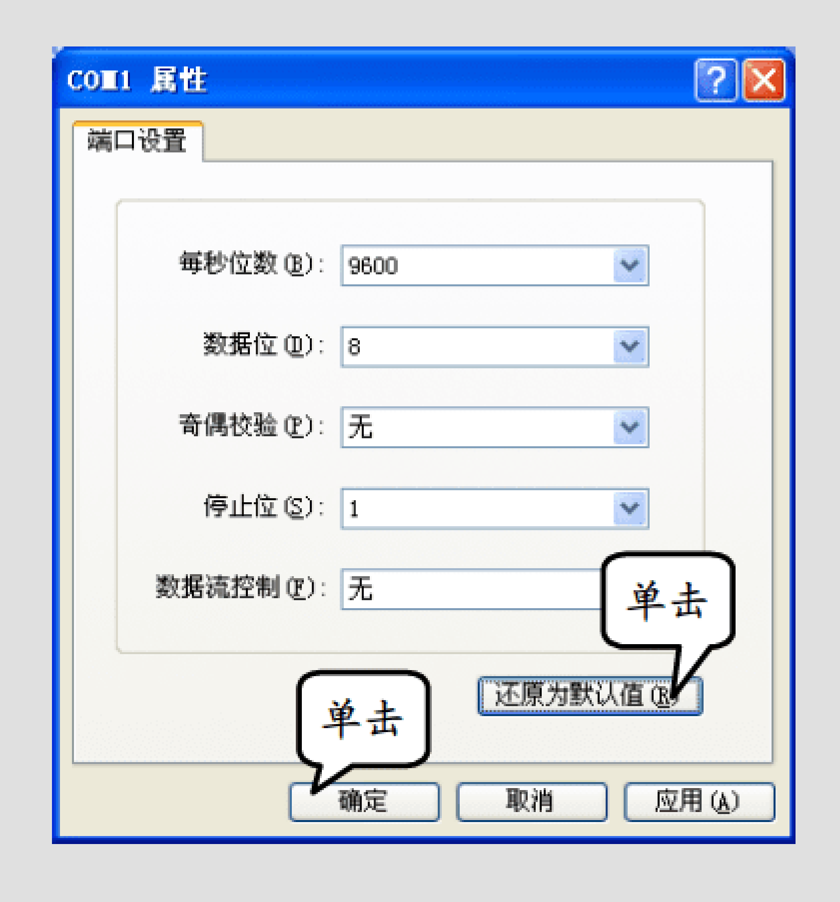


图 7-11　设置终端参数

（5）拨掉交换机的电源。

（6）接上电源，按住前面板的 mode 按钮不放，等 3～5 秒后松开 mode 按钮。可以看到如下提示。

```
The system has been interrupted prior to initializing the flash file system.
The following commands will initialize the flash file system, and finish loading
the operating system software:
flash_init
load helper
boot
```

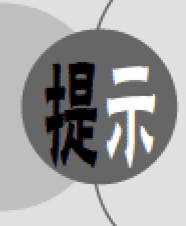
（7）在超级终端中输入 flash init 命令（初始化 flash 文件系统），并按回车键。

（8）输入 dir flash：命令，并按回车键。



通过 dir flash 命令，可以确认闪存内的配文件名为 config.text。

（9）输入 rename flash:config.text flash:config.old 命令（将配置文件重命名）按回车键，输入 boot 命令（重启交换机），并按回车键。



由于修改了配置文件，所以交换机找不到原配置文件(config.text)，从而出现配置的对话向导，选择 n 然后回车，这样就会绕过原来的 password 而进入用户模式。

（10）在用户模式输入 enable 命令，按回车键进入特权模式，并输入 rename flash:config.old

flash:config.text（复交换机配置文件）命令，按回车键。

（11）输入 copy flash:config.text system:running-config 命令（将原配置文件写入内存），并按回车键。

（12）在全局配置模式下，输入 no enable secret 命令（删除以前的密码），并按回车键，接着输入 enable secret 951753741 命令，并按回车键。



enable secret 951753741 设立新密码为 951753741。

（13）最后输入 exit 命令，按回车键，再输入 copy run start 命令，并按回车键。



命令 exit 可以退出当前模式，copy run start 是把当前配置文件写入闪存。

7.5.2 操作实例——华为交换机防止同网段 ARP 欺骗攻击

在交换机上配置端口与计算机 MAC 地址绑定，可有效防止 ARP 攻击造成的内网计算机网关欺骗和路由器 ARP 表错误。在此，使用“Cisco Packet Tracer”进行防止 ARP 欺骗攻击的配置，其配置方法与真实环境相同。

1. 实例目的

- 配置端口安全模式。
- 配置端口为接入层端口。
- 交换机端口与 MAC 地址绑定。

2. 实例步骤

（1）实验拓扑，如图 7-12 所示。

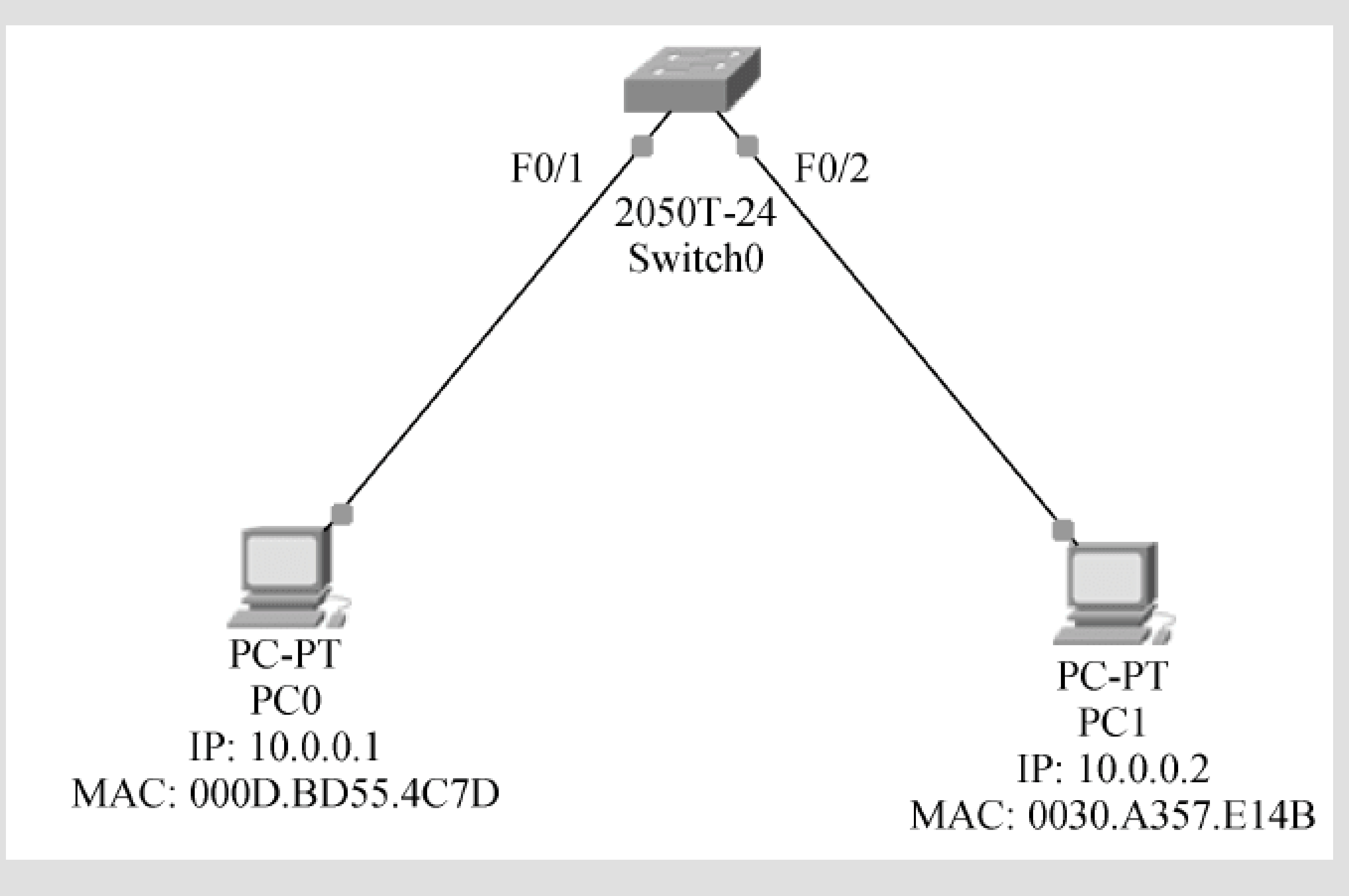


图 7-12　实验拓扑图

（2）使用图 7-12 说明在华为交换机上，防止同网段 ARP 欺骗攻击的基本配置，将计算机 0 的 MAC 地址与 Switch0 的 f0/1 端口绑定，计算机 1 的 MAC 地址与 Switch0 的 f0/2 端口绑定。

（3）在 Switch0 窗口 CLI 选项卡中，按回车键，进入用户模式，输入 enable 命令，按回车键，进入特权模式，如图 7-13 所示。

（4）在特权模式下输入 configure terminal（进入全局配置模式）命令，按回车键，如图 7-14 所示。

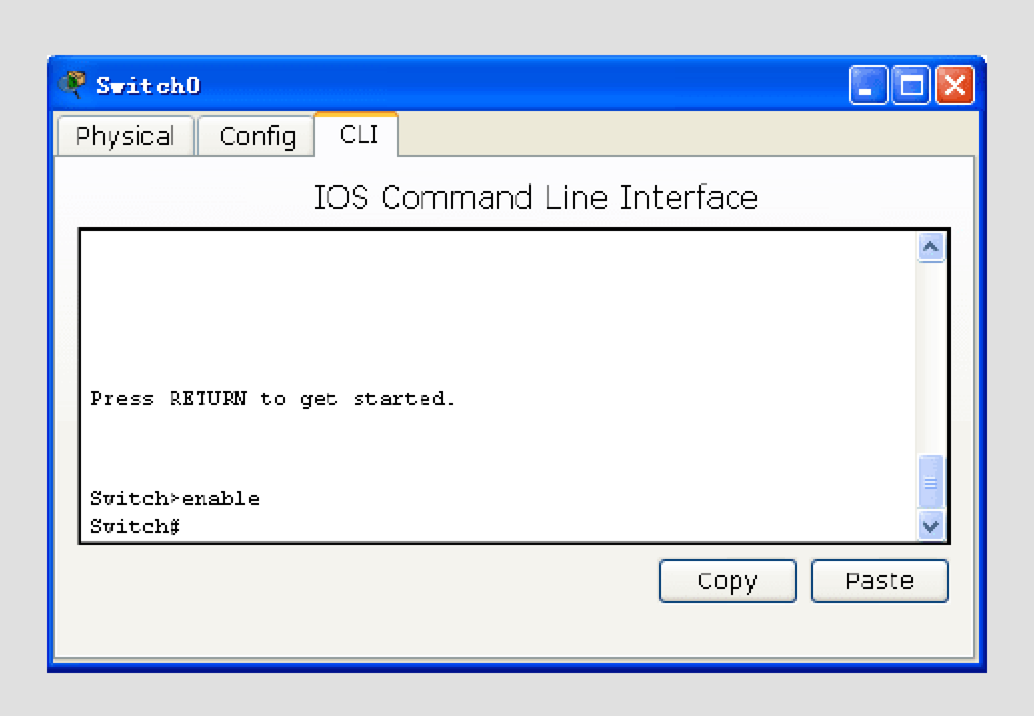




图 7-13　进入特权模式

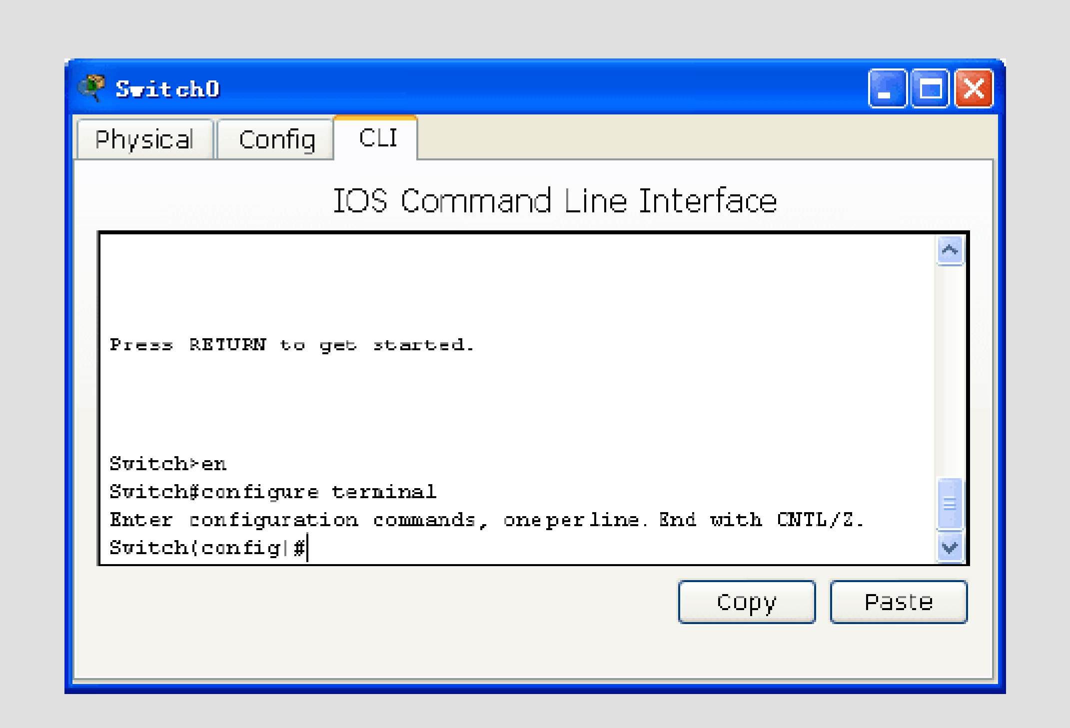


图 7-14　进入全局配置模式

（5）在全局配置模式下，输入 interface f0/1（进入 f0/1 接口模式）命令，按回车键，如图 7-15 所示。

（6）在接口模式下，输入 switchport mode access（配置端口为接入端口）命令，按回车键，如图 7-16 所示。

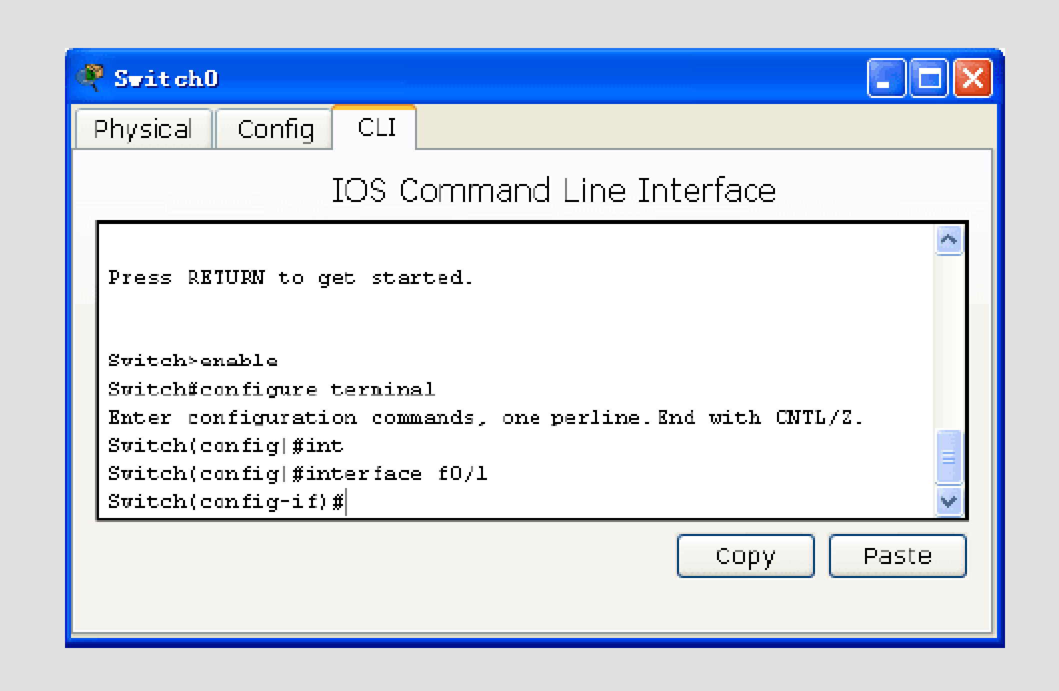


图 7-15　进入接口模式

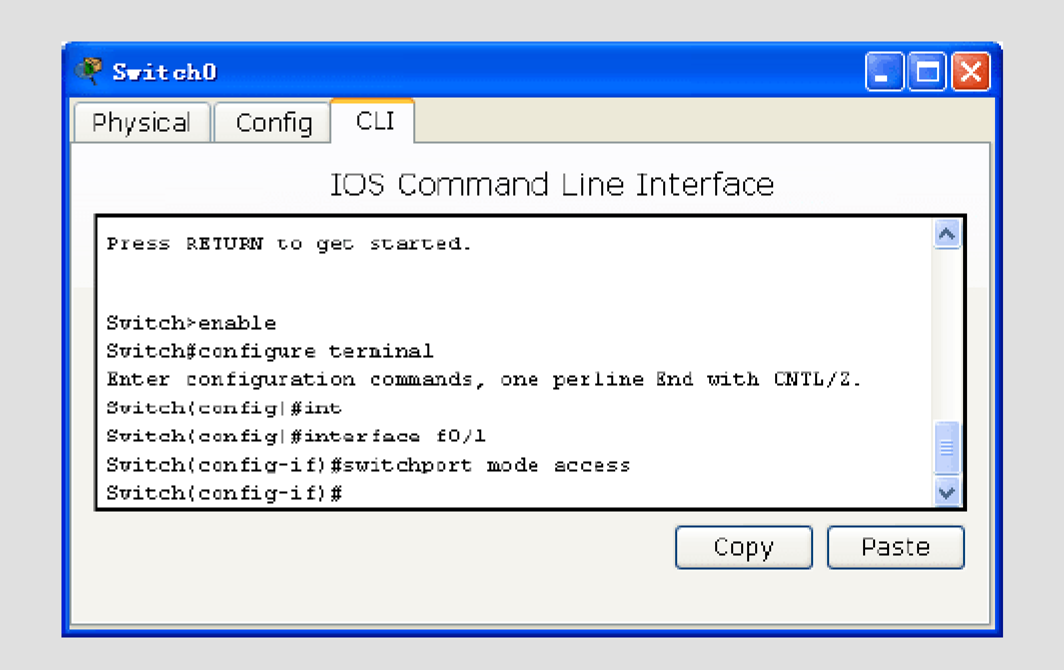


图 7-16　配置端口为接入端口

（7）在端口模式下输入 switchport port-secruity（进入端口安全模式）命令，按回车键，如图 7-17 所示。

（8）在端口安全模式下，输入 switchport port-security mac-address 000D.BD55.4C7D 命令，按回车键，如图 7-18 所示。

（9）在该模式下输入 interface f0/2（进入 f0/2 接口模式）命令，按回车键，如图 7-19 所示。

（10）在接口模式下，输入 switchport mode access （配置端口为接入端口）命令，按回车

键，如图 7-20 所示。

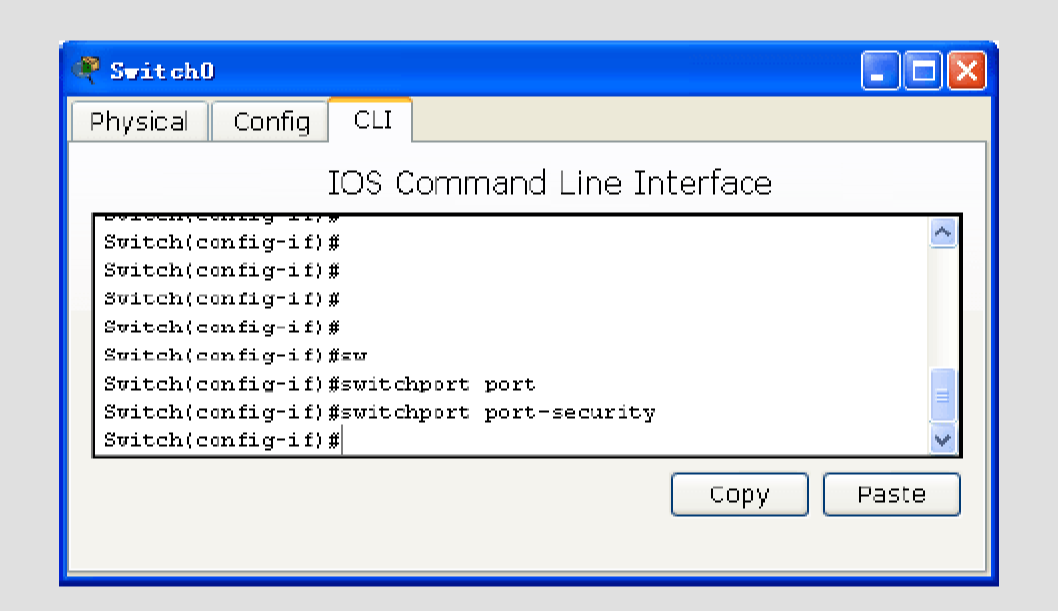


图 7-17　配置端口安全模式

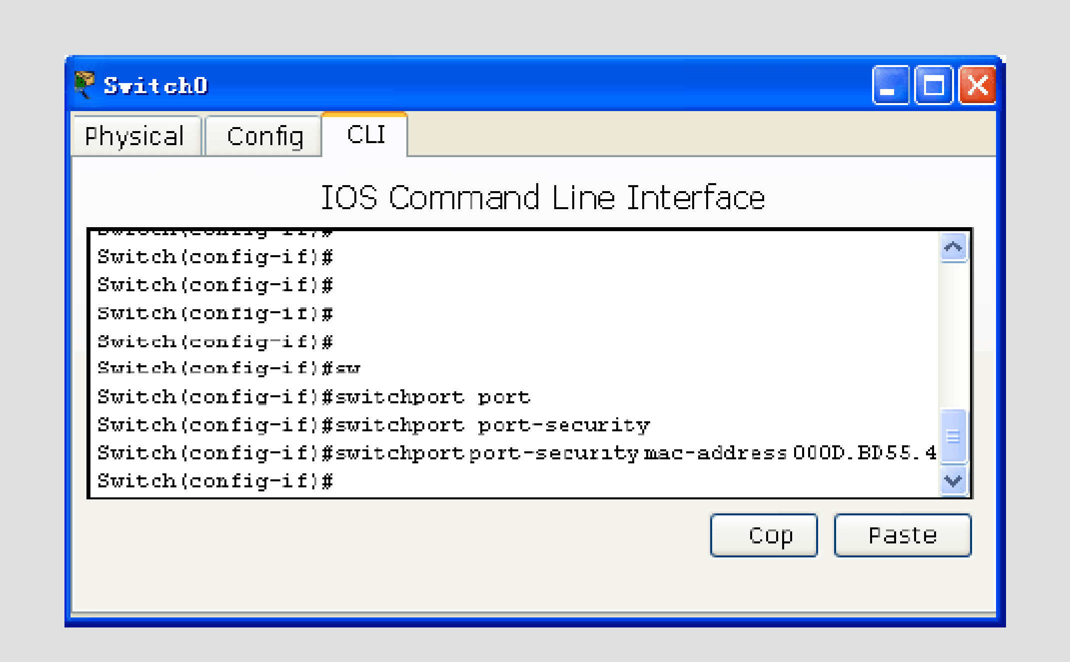


图 7-18　f0/1 端口与 MAC 地址绑定

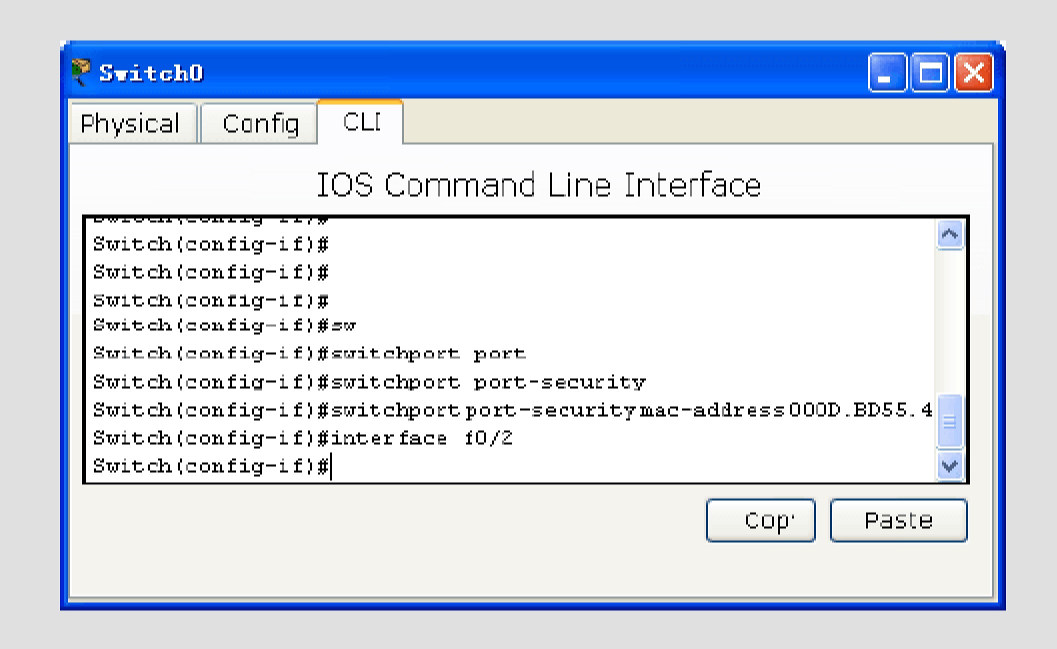


图 7-19　进入 f0/2 接口

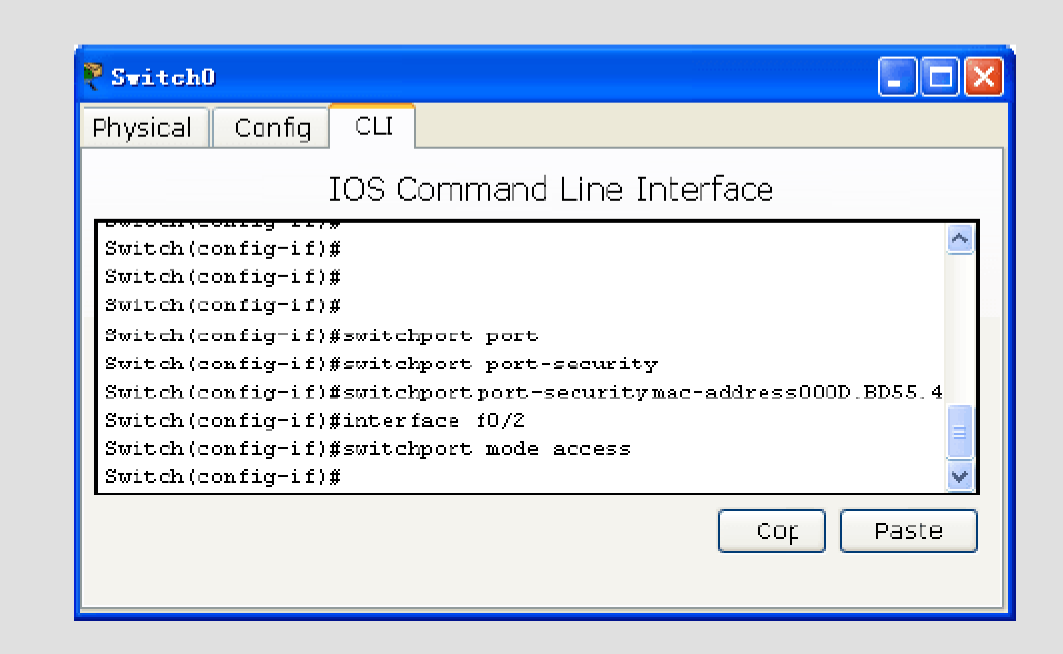


图 7-20　配置端口为接入端口

（11）在端口模式下输入 switchport port-security（进入端口安全模式）命令，按回车键，如图 7-21 所示。

（12）在端口安全模式下输入 switchport port-security mac-address 0090.0C27.968E 命令，按回车键，如图 7-22 所示。

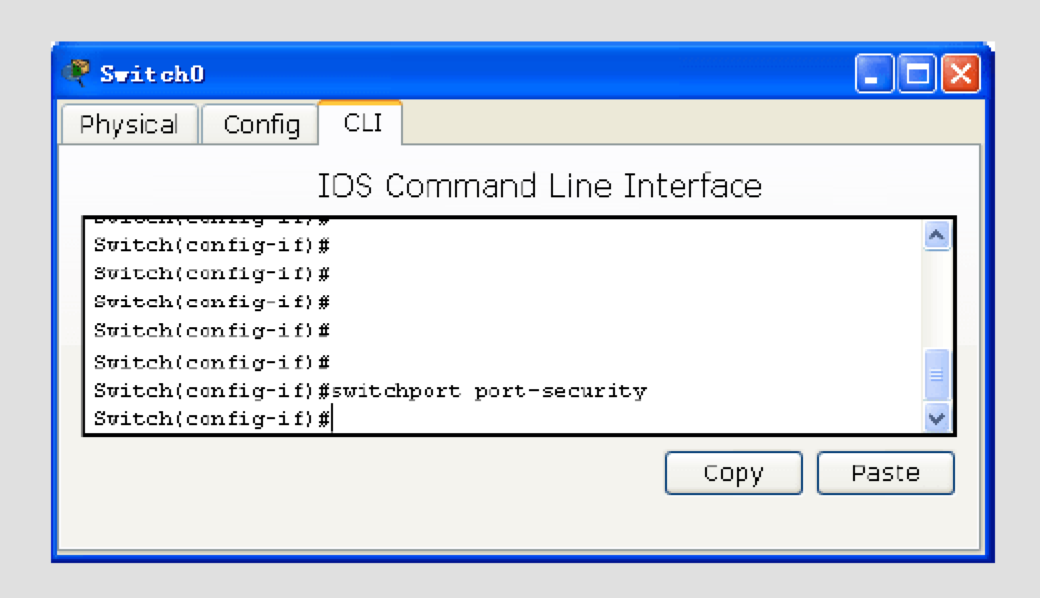


图 7-21　进入端口安全模式

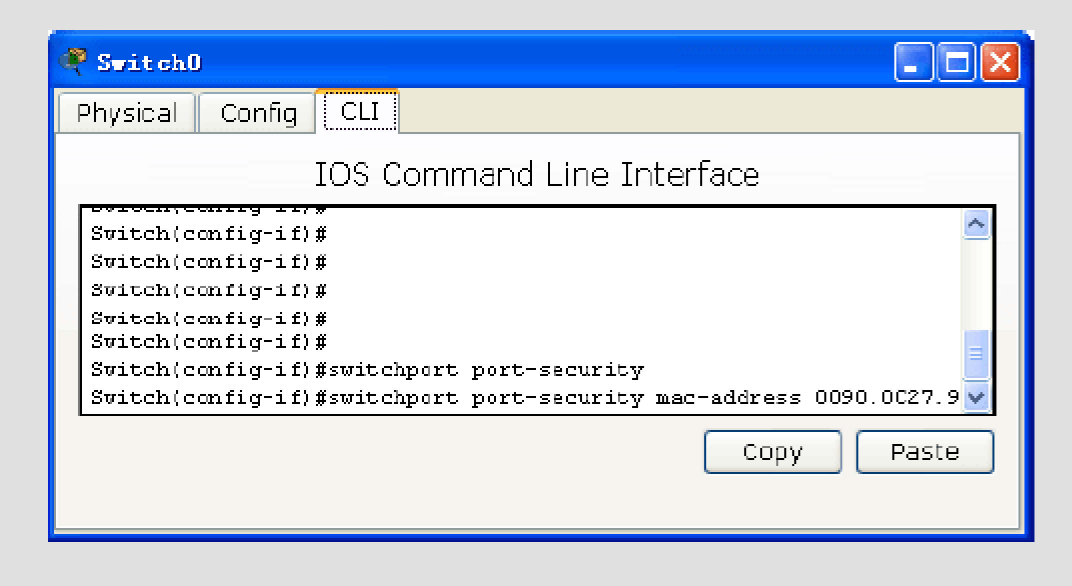


图 7-22　f0/2 端口与 MAC 地址绑定

（13）在特权模式下，输入 show mac-address table 命令，按回车键，如图 7-23 所示。

（14）将计算机 PC1 与 f0/1 相连，PC0 与 f0/2 相连，网络无法通信，如图 7-24 所示。

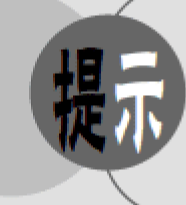


图 7-24 中节点颜色若为绿色表示网络可以正常通信，节点颜色若为红色表示网络不能正常通信。

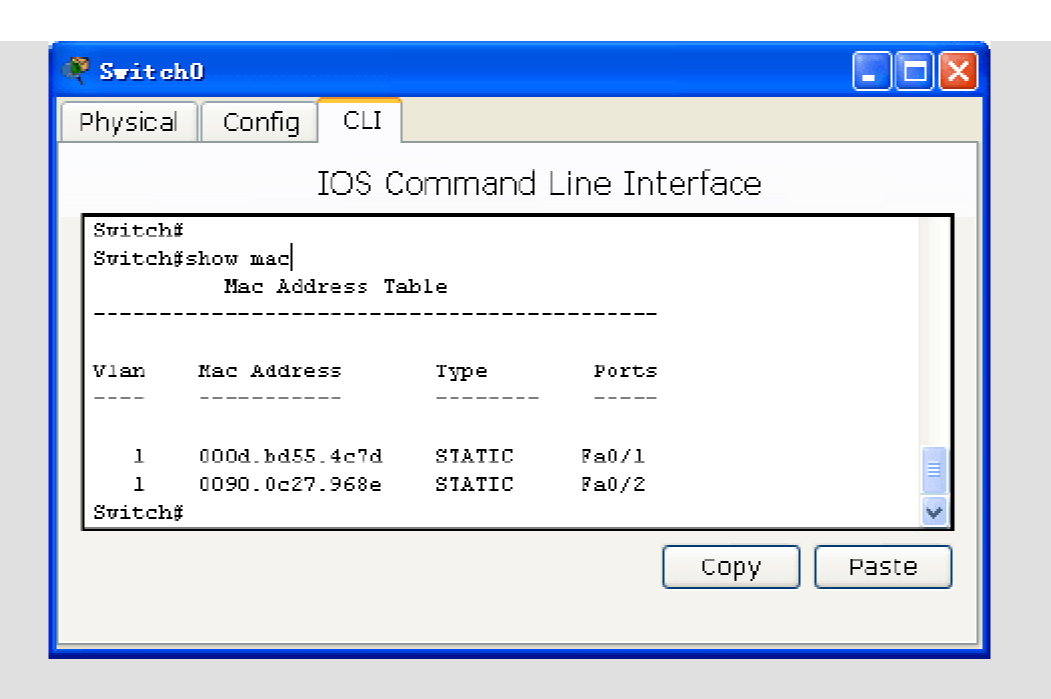


图 7-23　查看 MAC 地址表

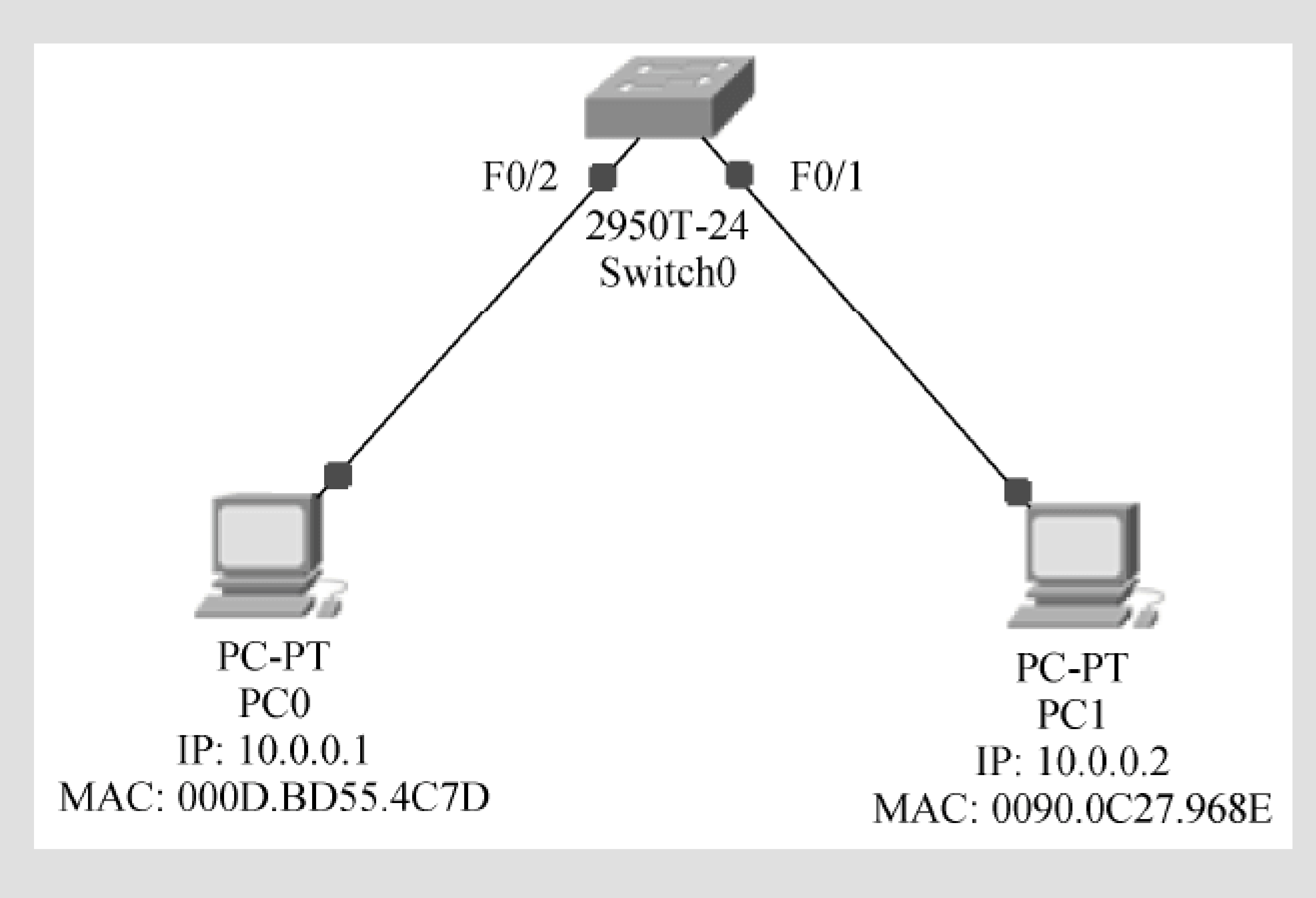


图 7-24　网络不能联通

第8章 路由器安全配置

随着路由应用的不断增加，路由器将逐步成为网络系统中不可缺少的重要部件，如果路由器连自身的安全都没有保障，那么整个网络也就毫无安全可言。

用户对于网络数据通信的安全性提出了更高的要求，诸如防范黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全性。但可能很多人还不了解如何进行路由器安全设置，才能提高网络的安全性。

因此在网络安全管理上，必须对路由器进行合理规划、配置，采取必要的安全保护措施，避免因路由器自身的安全问题而给整个网络系统带来漏洞和风险。本章介绍访问列表安全配置、网络地址转换技术及网络攻击安全防范一些加强路由器安全的措施和方法，让网络更安全。

本章学习要点：

- 了解并掌握访问列表安全及配置
- 掌握网络地址转换
- 熟悉网络攻击安全防范
- 了解使用 SDM 配置路由器

8.1 访问列表安全

访问控制列表（Access Control List，ACL）是 Cisco IOS 提供的一种访问控制技术，被广泛应用于路由器和三层交换机中。其目的是对网络数据通信进行过滤，从而实现各种访问控制需求。

ACL 技术通过数据包中源 IP 地址、目标 IP 地址、协议号、源端口号和目标端口号这 5 个元素来区分特定的数据流，并对匹配预设规则的数据采取相应的措施，允许（Permit）或拒绝（Deny）数据通过，从而可以有效地控制用户对网络和 Internet 的访问，最大限度地保障网络安全，使得企业网络不被滥用。

8.1.1 访问列表概述

ACL 使用包过滤技术，在路由器上读取网络层及传输层报头中的信息，如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对数据包进行过滤，从而达到访问控制的目的。

不过，由于 ACL 是通过利用包过滤技术来实现的，过滤的依据又仅仅是网络层和传输层报头中的部分信息，因此这种技术具有一些固有的局限性，如无法识别到具体的用户或应用到内部的权限类别等。所以，要达到“端到端”（传输层之间通信）的权限控制目的，则需要和系统级及应用级的访问权限控制结合使用。

1．访问列表类型

通常，应用在路由器上的 ACL 包括 IP 访问列表、MAC 访问列表、时间访问列表和 VLAN 访问列表等，而在 IP 访问列表中，又可细分为标准 IP 访问列表、扩展 IP 访问列表、VLAN ACL 和命名 ACL 四部分。

❑ **IP 访问列表**

过滤 IP 通信，包括 TCP、User Datagram Protocol（UDP）、Internet Group Management Protocol（IGMP）和 Internet Control Message Protocol（ICMP）。

❑ **MAC 访问列表**

对进入二层接口的通信实施访问控制，也称为端口访问列表。

❑ **时间 ACL**

基于不同时间段对网络实施控制。

❑ **VLAN 访问列表**

对所有数据包实现访问控制。在同一 VLAN 的设备之间，可以采用 VLAN ACL 实施访问控制。它与访问控制均基于 IP 地址，不支持基于 MAC 地址的访问控制。

❑ **标准 IP 访问控制列表**

标准访问列表只允许过滤源地址，且功能十分有限。当要想阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者想要拒绝某一协议簇的所有通信流量时，可以使用标准访问控制列表来实现这一目标。标准访问控制列表检查路由的数据包的源地址，从而允许或拒绝基于网络、子网或主机的 IP 地址的所有通信流量通过路由器的出口。

❑ **扩展 IP 访问控制列表**

扩展访问列表允许过滤源地址、目的地址和上层应用数据，因此，可以适应各种复杂的网络应用。扩展访问控制列表，不仅可以检查数据包的源地址、检查数据包的目的地址，还可检查数据包的特定协议类型、端口号等。扩展访问控制列表更具有灵活性和可扩充性，即可以对同一地址允许使用某些协议通信流量通过，而拒绝使用其他协议的流量通过。

❑ **命名访问控制列表**

在标准与扩展访问控制列表中均需要使用列表编号，而在命名访问控制列表中，使用一个字母或数字组合的字符串来代替前面所使用的数字。使用命名访问控制列表，可以用来删除某一条特定的控制条目。这样，可以在使用过程中方便地对访问列表进行修改。

2．配置访问列表应注意的问题

配置访问列表时，应对配置列表需要遵循的原则、列表被处理的顺序、列表存放的位置及列表应用等方面作相关了解。

❑ **遵循最小特权原则**

在设置访问列表时，应当遵循最小特权原则，即只给受控对象完成任务所必须的最小的权限，从而最大限度地保障网络传输安全。最小特权（Least Privilege）是指在完成某种操作时所赋予网络中每个主体（用户或进程）必不可少的特权。最小特权原则是指应限定网络中每个主体所必须的最小特权，确保可能发生的事故、错误、网络部件的篡改等原因造成的损失最小。最小特权原则一方面给予主体必不可少的特权，保证所有的主体都能在所赋予的权限内完成自己的任务或操作；另一方面，只给予主体必不可少的特权，从而限制每个主体所能进行的操作，以确保企业网络安全。

❑ **自上而下的处理过程**

在访问列表中，包含一个访问控制条目（Access Control Entry，ACE）规则列表，每个ACE 都指定"permit"（允许）或"deny"（拒绝）及应用条件，数据包会逐个条目顺序匹配ACE。访问列表内，表项的检测按自上而下的顺序进行，且从第一个表项开始。这意味着必须特别谨慎地考虑访问列表中语句的顺序。

➢ **添加表项**　新增加的表项被追加到访问列表末尾，这将决定不能改变已有的访问列表的功能。如果要改变，就必须创建一个新的访问列表，并删除已经存在的访问列表，然后将新的访问列表应用于接口上。
➢ **标准访问列表过滤**　标准访问列表只限于过滤源地址。因此，通常需要使用扩展的 IP 访问列表来满足企业的特殊需求。
➢ **访问列表位置**　应当将扩展访问列表尽量放在靠近过滤源的位置上，这样创建的过滤器就不会反过来影响其他接口上的数据流。而标准访问列表则应当尽量靠近目的位置，由于标准访问列表只使用源地址，因此将阻止报文流向其他端口。
➢ **语句的位置**　由于 IP 协议包含 ICMP、TCP 和 UDP，所以，应当将具体的表项放在不太具体的表项前面，保证更加准确进行数据的筛选。
➢ **访问列表应用**　使用 Access-group 命令应用访问列表，但需要注意的是，只有访问列表被应用于接口上时，才执行过滤操作，从而真正产生作用。
➢ **过滤方向**　通过接口的数据流是双向的。过滤方向定义了想要检查的是流入还是流出的报文。所以，访问列表要应用到接口的特定方向上。向外的（Outbound），表示数据流从三层设备流出；向内的（Inbound），表示数据流流向三层设备。

3. 访问列表配置步骤

❑ 分析需求，找出需求中要保护什么或控制什么（为方便配置，最好能以表格形式列出）。
❑ 编写 ACL 规则。
❑ 根据需求与网络结构，将规则应用于路由器或交换机的特定接口上。

8.1.2 IP 访问列表

针对 IP 访问列表过滤对象和配置元素的不同，可将其分为标准 IP 访问列表、扩展 IP 访问列表及名称 ACL3 种类型。

1. 标准 IP 访问列表

标准 IP 访问列表中，对数据的检查元素仅是源 IP 地址。图 8-1 所示为基于标准 IP 访问列表进行数据包过滤的网络结构，在该例中，要求 172.16.1.0 网段的计算机不可以访问服务器 172.17.1.1，而其他计算机访问该服务器时则不受限制（需求分析）。

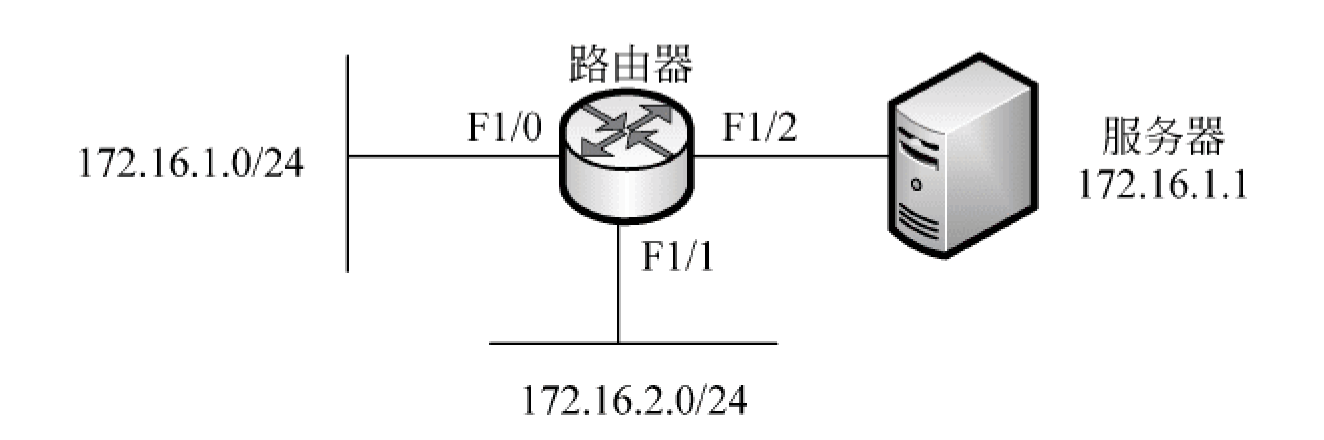


图 8-1　标准 IP 访问列表

明确该实例网络需求后，则可依据该需求编写标准 IP 访问列表规则。其配置命如下所示。

```
access-list access-list-number {permit|deny} {any|source source-wildcard}
[time-range time-range-name]
```

- **access-list-number**　所创建的标准 ACL 编号，其范围是 1~99 和 1300~1999。
- **permit|deny**　对匹配此规则的数据包采取的措施，permit 表示允许数据包通过，deny 表示拒绝数据包通过。
- **any**　any 表示任何源地址。
- **source**　需要检测的源 IP 地址或网段，如在本例中，检测的源 IP 地址网段为 172.16.1.0。
- **source-wildcard**　source-wildcard 表示与需要检测的源 IP 地址匹配的反向子网掩码。这里需要注意的是，此处是反掩码，例如需要检测的源 IP 地址网段为 172.16.1.0，相对应的反掩码为 0.0.0.255，反掩码也称为通配符，和子网掩码相反。这里，转化为二进制后，为 0 的项是需要匹配的项，为 1 的项是不需要匹配的项。
- **time-range time-range-name**　规则生效的时间范围，并指定时间范围的名称。

在本例中，只需要过滤源 IP 地址属于 172.16.1.0 网段的数据，因此源 IP 地址的前 3 个字段为需要检测的字段，ACL 规则如下所示：

```
access-list 1 deny 172.16.1.0 0.0.0.255
```

在配置 ACL 时需要注意的是，ACL 中，默认的规则是拒绝所有。也就是说，在上述访问列表中只有一条拒绝 172.16.1.0 网段的规则，但实际在该规则后还有一条隐含的规则：access-list deny any。ACL 的检查原则是自上而下，逐条匹配，一旦匹配成功就执行动作，若访问列表中的所有规则都不匹配，则执行默认规则“拒绝所有”。例如，本例中的访问列表规则将拒绝所有的数据流量，所以编写访问列表规则的时候，一定要注意最后的默认“拒绝所有”规则。在本例中，可以在拒绝的规则后加上一条规则。

```
access-list 1 deny 172.16.1.0 0.0.0.255
access-list 1 permit any
```

编写好的访问控制列表需要应用到相应的端口上才会生效。在端口模式下，使用如下命令应用 ACL。

```
ip access-group access-list-number {in|out}
```

- **access-list-number**　该数字为需要在该端口应用的访问列表的编号。例如，本例中此编号为 1。
- **in|out**　in|out 表示在该端口上是对哪个方向的数据进行过滤，in 表示对进入该端口的数据进行过滤，out 则表示对从该端口发出的数据进行过滤。

另外，在应用标准 IP ACL 时，通常将其放置到尽可能靠近目标的位置。例如在本例中，如果将 ACL 应用在靠近源端口 f1/0，那么网段 172.16.1.0 内的计算机除了可以访问到本网段的计算机外，其他任何网络都访问不到。因此，在该例中 ACL 最合适的放置位置是端口 f1/2 上。ACL 规则编写及应用的配置命令如下。

```
Router#configure terminal
Router(config)#access-list 1 deny 172.16.1.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#interface fastethernet 1/2
Router(config-if)#ip access-group 1 out
Router(config-if)#end
Router# copy running-config startup-config
```

2. 扩展 IP 访问列表

从标准 IP 访问列表中，可看到利用访问控制能够限制网络中的计算机去访问特定的资源。但假定连接在路由器 f1/2 端口上的是一个服务器群，除服务器 172.17.1.1 外，还有服务器 172.17.1.2，如图 8-2 所示。

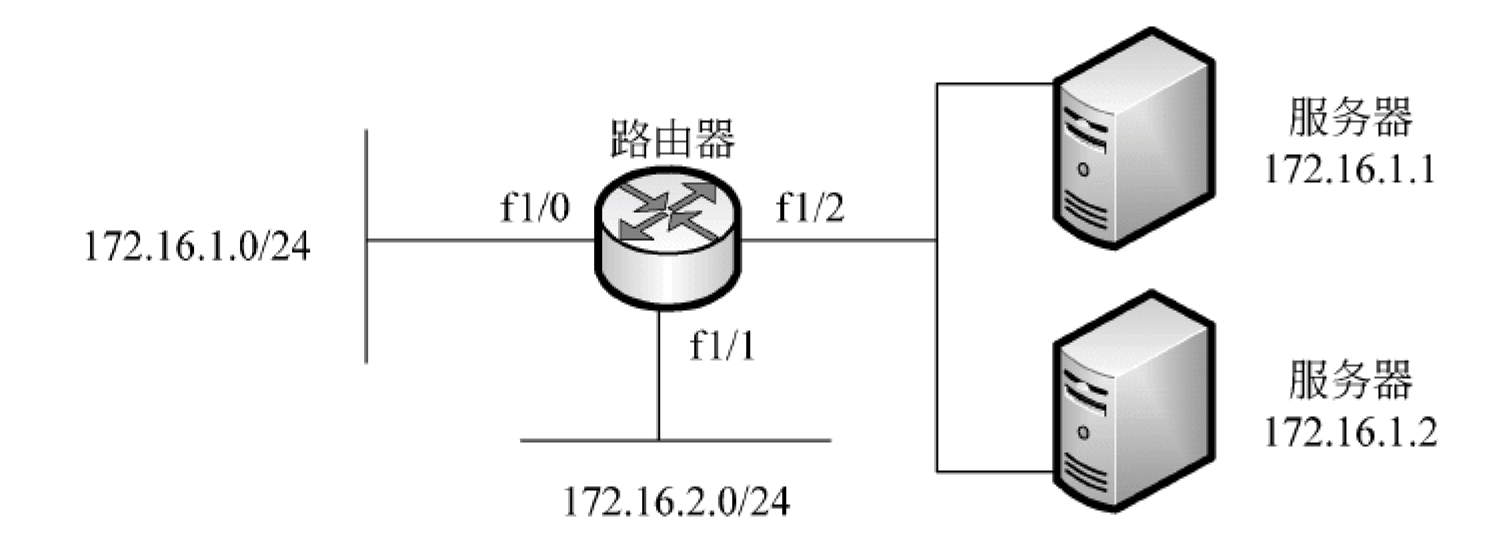


图 8-2　扩展 IP 访问列表

显然，使用标准 IP 访问列表将无法实现此需求，因为将标准 IP 访问列表应用到 f1/2 端口上，会导致两台服务器都不能被访问。在这种情况下，就需要用到扩展 IP 访问列表。扩展 IP 访问列表与标准 IP 访问列表的应用规则基本相同，差别只在于扩展的访问控制列表对数据的检查元素更丰富一些。扩展 IP 访问列表，可检查的元素包括源 IP 地址、目标 IP 地址、协议、源端口号、目标端口号。

若要在图 8-2 所示网络结构中，实现 172.16.1.0 网段的计算机不可以访问服务器

172.17.1.1，而其他计算机访问该服务器时则不受限制这一要求，则需要同时对数据包的源 IP 地址和目标 IP 地址进行检查（需求分析）。

对需求进行分析后，可依据需求编写扩展 IP 访问列表规则。其配置命令如下所示。

```
access-list access-list-number {deny|permit} protocol {any|source source-wildcard} [operator port] {any|destination destination-wildcard} [operator port] [precedence precedence] [tos tos] [time-range time-range-name] [dscp dscp] [fragment]
```

- **access-list-number**　所定义的扩展 IP 列表的编号，其范围为 100~199 和 2000~2699。
- **deny|permit**　指定对匹配此规则数据包的处理方式，deny 表示拒绝，permit 表示允许。
- **protocol**　协议，如 IP、ICMP、TCP、UDP 等。
- **any**　any 表示任何源地址。
- **source**　数据包的源 IP 地址。
- **source-wildcard**　源 IP 地址的反掩码。
- **operator**　源端口操作符，lt 表示小于，eq 表示等于，gt 表示大于，neg 表示不等于，range 表示范围。只有 protocol 为 TCP 或 UDP 时，才会有此项。
- **port**　源端口号，可以使用数字或服务器名称表示，如 www、ftp 等。
- **any**　表示任何目标地址。
- **destination**　数据包的目标 IP 地址。使用“any”表示任何目标地址。
- **destination-wildcard**　目标 IP 地址的反掩码。
- **operator**　目标端口操作符，lt 表示小于，eq 表示等于，gt 表示大于，neg 表示不等于，range 表示范围。只有 protocol 为 TCP 或 UDP 时，才会有此项。
- **port**　目标端口号，可以使用数字或服务器的名称表示，如 www、ftp 等。
- **precedence**　报文的 IP 优先级别，范围 0~7。
- **tos tos**　报文的服务类型，范围为 0~15。
- **time-range time-range-name**　规则生效的时间范围，并指定时间范围的名称。
- **dscp dscp**　数据包的 DSCP（Differentiated Services Code Point）值，范围为 0~64。
- **fragment**　fragment 表示非初始分段报文。当使用这个参数后，此 ACL 规则将只会对未被分段的报文进行检查，而不检查在数据传输过程中已分段的报文。

在端口应用扩展 IP 访问列表的方式，与标准 IP 访问列表一样。由于扩展 IP 访问列表对数据的检测可以做得更精确，因此 ACL 规则可以应用在靠近源端位置。这里在路由器 f1/0 端口，按照如下命令配置和应用扩展 IP ACL，将不会带来 172.16.1.0 网段的计算机无法访问任何网络的问题，只是不能访问服务器 172.17.1.1。

```
Router#configure terminal
Router(config)#access-list 100 deny ip 172.16.1.0 0.0.0.255 host 172.17.1.1
Router(config)#access-list 100 permit ip any any
Router(config)#interface fastethernet 1/0
Router(config-if)#ip access-group 100 in
Router(config-if)#end
Router# copy running-config startup-config
```

在上面网络需求中，只用指定目标地址就可以满足要求。但在另一些需求中，可能还需要指定端口。例如，172.17.1.1 为公司的文件服务器，要求网段 172.16.1.0 中的计算机能够访问 172.17.1.1 中的 FTP 服务和 Web 服务，而对服务器上其他服务禁止访问。此时，则需要按照以下命令进行扩展 IP ACL 规则的配置和应用。

```
Router#configure terminal
Router(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 172.17.1.1
eq www
Router(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 172.17.1.1
eq ftp
Router(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 host 172.17.1.1
eq eq ftp-date
Router(config)#access-list 100 permit ip 172.16.1.0 0.0.0.255 host 172.17.1.2
Router(config)#access-list 100 permit ip any
Router(config)#interface fastethernet 1/0
Router(config-if)#ip access-group 100 in
Router(config-if)#end
Router# copy running-config startup-config
```

在上面配置命令中，www 表示端口号 80，ftp 表示 FTP 的控制端口 21，ftp-data 表示 FTP 的数据端口 20。而此例中，没有指定源端口号，因为这里只关心目标端口（若不指定源端口，则表示匹配所有源端口）。另外，由于 ACL 的默认操作为拒绝所有，所以最右面的拒绝其他所有流量的规则可省略。

3. 名称 ACL

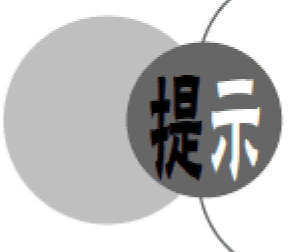
标准 IP ACL 和扩展 IP ACL 均属于编号访问控制列表，且它们的编号范围分别为 1~99 和 1300～1999、100～199 和 2000～2699，有耗尽的可能，而名称 ACL 则没有这种限制。除了在编写规则的语法上稍有不同，其他诸如检查元素、默认规则等均与编号访问列表相同。另外，名称 ACL 同样分为标准 IP ACL 和扩展 IP ACL。

❑ **标准名称 IP ACL**

在全局配置模式下，使用如下命令可创建并配置标准名称 IP ACL。

```
ip access-list standard {name|access-list-number}
```

在该命令中，name 字段指定此 ACL 的名称，可使用数字或英文字母表示。执行完此命令后，系统将进入标准 ACL 配置模式；access-list-number 字段表示标准名称 ACL 的编号，其范围为 1～99 和 1300～1999。



当这里指定 ACL 的编号而不指定名称时，此 ACL 将是一个编号 ACL，与之前介绍的标准 ACL 一样，但在配置标准名称 ACL（带编号的）规则中，将会在 ACL 配置模式下进行。

在 ACL 模式下，可使用如下命令配置标准名称 ACL 规则（命令中参数的含义与编号 ACL

中相同）。

```
{permit|deny} {any|source source-wildcard} [time-range time-range-name]
```

❑ **扩展名称 IP ACL**

在全局配置模式下，使用如下命令可创建并配置扩展名称 IP ACL（命令中参数含义与标准名称 ACL 中相同）。

```
ip access-list extended {name|access-list-number}
```

在 ACL 模式下，可使用如下命令配置标准名称 ACL 规则（命令中参数的含义与编号 ACL 中相同）。

```
{permit|deny} protocol {any|source source-wildcard} [operator port] {any|
destination destination-wildcard} [operator port] [time-range time-range-name]
[dscp dscp] [fragment]
```

在端口应用名称 ACL 与应用编号 ACL 的方式和命令类似，只需要将编号替换为名称即可。

```
ip access-group name {in|out}
```

若要满足网段 172.16.1.0 内的计算机，能够访问文件服务器（IP 地址为 172.17.1.1）中 FTP 服务和 Web 服务，而对服务器上其他服务禁止访问这一要求。此时，可按照以下命令进行扩展名称 IP ACL 规则的配置和应用。

```
Router#configure terminal
Router(config)#ip access-list extended allow_ftp_web
Router(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 172.17.1.1 eq www
Router(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 172.17.1.1 eq ftp
Router(config-ext-nacl)#permit tcp 172.16.1.0 0.0.0.255 host 172.17.1.1 eq
ftp-data
Router(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 host 172.17.1.2
Router(config-ext-nacl)#exit
Router(config)#interface fastethernet 1/0
Router(config-if)#ip access-group allow_ftp_web in
Router(config-if)#end
Router# copy running-config startup-config
```

8.1.3　时间访问列表

在所介绍的各种 ACL 的规则配置中，可看到每种 ACL 规则后面都有一个可选的参数 time-range，此参数表示一个时间段。在实际的网络控制中，不同的时间段内需要不同的控制，例如学校网络中，希望上课时间禁止学生访问学校的某影视服务器，而下课时间则允许访问。这种情况下，ACL 需要和时间段结合起来应用，即基于时间的 ACL。事实上，基于时间的 ACL 只是在 ACL 规则后面使用 time-range 参数为此规则指定一个时间段，只有在此时间范围

内该规则才会生效，各类 ACL 均可以使用时间段。

时间段可分为绝对时间段（Absolute）、周期时间段（Periodic）和混合时间段 3 种类型。

- **绝对时间段**　绝对时间段表示一个时间范围，即从某时刻开始到某时刻结束，例如 1 月 5 日早晨 8 点到 3 月 6 日早晨 8 点。
- **周期时间段**　周期时间段表示一个时间周期，例如每天的早晨 8 点到晚上 6 点，或每周一至周五的早晨 8 点到晚上 6 点。也就是说，周期时间不是一个连续的时间范围，而是特定某天的某个时间段。
- **混合时间段**　可以将绝对时间段和周期时间段结合应用，称为混合时间段。例如，1 月 5 日到 3 月 6 日的每周一到周五早晨 8 点到晚上 6 点。

1．创建时间段

在全局配置模式下，使用如下命令创建并配置时间段。

```
time-range time-range-name
```

- **time-range-name**　表示时间段的名称。执行该命令后，系统将进入时间段配置模式。

2．配置绝对时间段

在时间段配置模式，使用如下命令配置绝对时间段。

```
absolute {start time date [end time date] | end time date}
```

- **start time date**　表示时间段的起始时间。time 表示时间，格式为“hh:mm”；date 表示日期，格式为“日、月、年”。
- **end time date**　表示时间段的结束时间，格式与起始时间相同。

在配置绝对时间段时，可以只配置起始时间或只配置结束时间。以下为 2009 年 1 月 1 日 8 点到 2010 年 2 月 1 日 10 点，使用绝对时间段范围表示的配置示例。

```
absolute start 8:00 1 Jan 2009 end 10:00 1 Feb 2010
```

3．配置周期时间段

在时间段配置模式下，使用如下命令配置周期时间段。

```
periodic day_of_the_week hh:mm to [day_of_the_week] hh:mm
periodic {weekdays|weekend|daily} hh:mm to hh:mm
```

- **day_of_the_week**　表示一个星期内的一天或几天，Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、Sunday。
- **hh:mm**　表示时间。
- **weekdays**　表示周一到周五。
- **weekend**　表示周六到周日。
- **daily**　表示周一到周日。

以下为每周一至周五早晨 9 点到晚上 18 点，使用周期时间段范围表示的配置示例。

```
periodic weekdays 09:00 to 18:00
```

4．应用时间段

配置完时间段后，必须在 ACL 规则中使用 time-range 参数引用时间段才能生效，且只有在 time-range 规则中指定的时间段内生效，其他未引用的时间段将不受影响。

图 8-3 所示为某公司的网络，现在需要配置访问控制规则，在上班时间（9：00～18：00）不允许员工的计算机（172.16.1.0/24）访问 Internet，下班时间可以访问 Internet 上的 Web 服务。

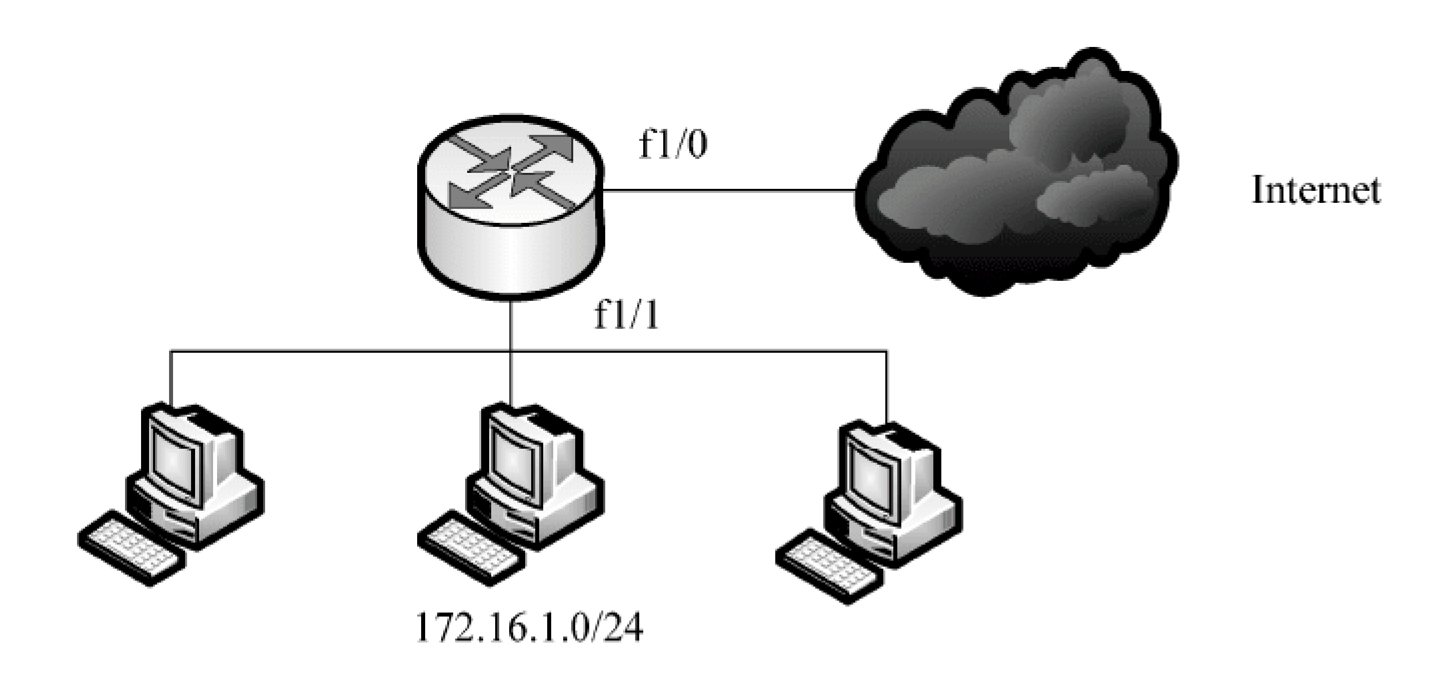


图 8-3　基于时间的 ACL

要实现该公司网络需求，可按照以下命令对时间 ACL 规则进行配置和应用。

```
Router#configure terminal
Router(config)#time-range off-work
Router(config-time-range)#periodic weekdays 09:00 to 18:00
Router(config-time-range)#exit
Router(config)#access-list 100 deny ip 172.16.1.0 0.0.0.255 any time-range off
work
Router(config)#access-list 100 permit tcp 172.16.1.0 0.0.0.255 any eq www
Router(config)#interface fastethernet 1/1
Router(config-if)#ip access-group 100 in
Router(config-if)#end
Router# copy running-config startup-config
```

在以上示例中，第 1 条规则为拒绝 172.16.1.0/24 内计算机访问 Internet，在此规则中引用了一个时间段“off-work”，即只有在该时间规则定义的时间范围内此控制才会生效，如果当前时间不在定义的时间范围内，则系统会跳过这条规则去检查下一条规则（下班时间可以访问 Internet 的 Web 服务），然后将此 ACL 应用到内部端口的入方向实施过滤。

在使用基于时间的 ACL 时，最重要是要保证设备（路由器或交换机）系统时间的准确性，因为设备是根据自己的系统时间来判断当前时间是否在时间段范围内的。为了保证设备系统时间的准确性，可以使用 NTP（Network Time Protocol，网络时间协议）来保证网络中时钟的同步，或在特权模式下，使用 clock set 命令调整系统时间，并利用 show clock 命令查看当前系统时间。

8.1.4 MAC 访问列表

所介绍的编号和名称的标准 ACL 和扩展 ACL 都是基于 IP 的，所以称为 IP ACL。但在某些场合基于 IP 的 ACL 可能无法满足网络的需求。例如，图 8-4 所示为一个企业网络，它只允许公司财务部的计算机（172.16.1.1）访问公司的财务服务器（172.16.1.254），不允许其他任何员工的计算机访问财务服务器。

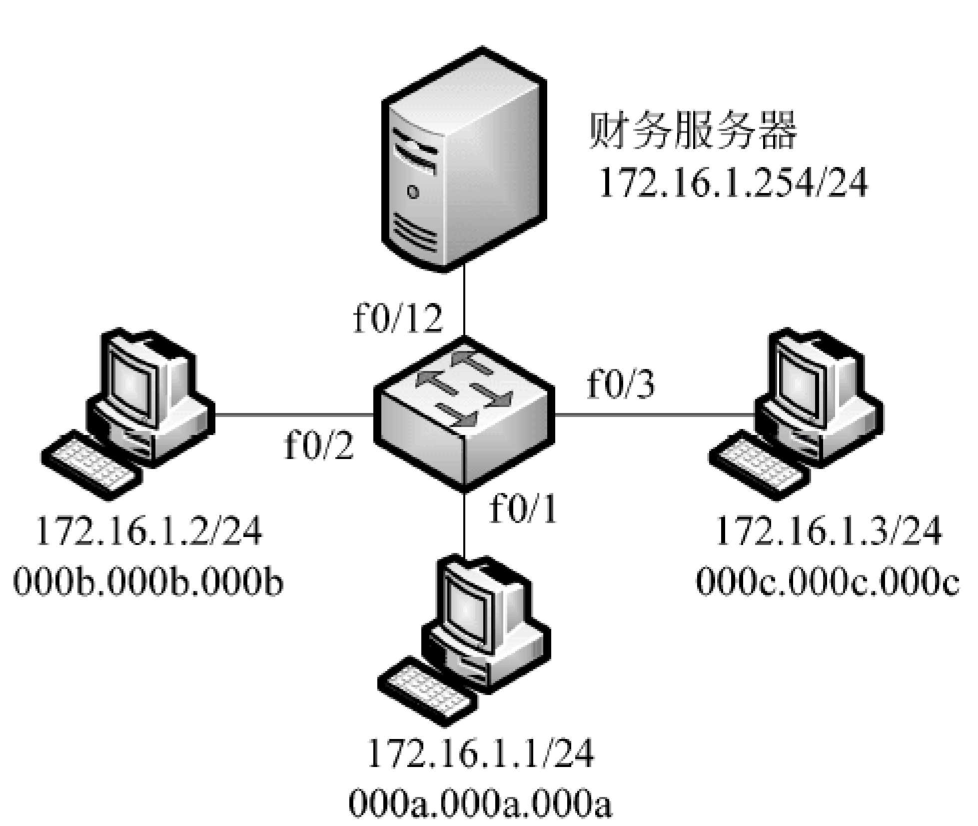


图 8-4 MAC 访问列表

对于以上需求，虽然也可以使用扩展 IP ACL 实现，但如果其他员工修改计算机的 IP 地址为 172.16.1.1，那么就能够访问财务服务器，这种情况下使用基于 MAC 的 ACL 则可以避免此现象的发生。因为，基于 MAC 的 ACL 所检查的元素为数据包的源 MAC 地址和目标 MAC 地址，而通常计算机的 MAC 地址是固定的，不能修改的，所以根据 MAC 地址过滤的访问控制设备不会被“欺骗”。

1. 配置 MAC ACL

在全局配置模式下，使用如下命令可创建并配置基于 MAC 的 ACL。

```
mac access-list extended {name|access-list-number}
```

- **name** 表示 MAC ACL 的名称。执行此命令后，系统将进入到 MAC ACL 配置模式。
- **access-list-number** MAC ACL 的编号，范围为 700~799。

进入 MAC ACL 模式后，使用如下命令配置 MAC ACL 的访问控制规则。

```
{permit|deny} {any|host source-mac-address} {any|host destionation-mac-
address} [ethernet-type] [time-range time-range-name]
```

- **permit|deny** 指定对符合此规则的数据包的处理方式，deny 为拒绝，permit 为允许。
- **any** 表示任何源 MAC 地址。
- **host source-mac-address** 表示源 MAC 地址。
- **any** 表示任何目标 MAC 地址。

- **host destination-mac-address** 表示目标 MAC 地址。
- **ethernet-type** 表示以太网类型。如果不指定，则表示匹配所有类型的以太网帧。
- **time-range time-range-name** 表示规则生效的时间范围，并指定时间范围的名称。

2. 应用 MAC ACL

在端口模式下，使用如下命令将 MAC ACL 应用到端口。

```
mac access-group {name|access-list-number} {in|out}
```

- **name** 表示 MAC ACL 名称。
- **access-list-number** 表示 MAC ACL 的编号，范围是 700~799。

对于 MAC ACL，一些交换机只支持入方向（in）的过滤，所以在配置和应用 MAC ACL 时，需要考虑 ACL 规则的配置方式，以及应用 MAC ACL 的端口。

在此，假设图 8-4 中财务服务器的 MAC 地址为 000d.000d.000d，且使用 MAC ACL 实现只允许财务部的计算机能够访问财务服务器。MAC ACL 被应用到接入非财务计算机端口的入方向。其配置如下所示。

```
Router#configure terminal
Router(config)#mac access-list extended deny_to_accsrv
Router(config-mac-nacl)#deny any host 000d.000d.000d
Router(config-mac-nacl)#permit any any
Router(config-mac-nacl)#exit
Router(config)#interface fastethernet 0/2
Router(config-if)#mac access-group deny_to_accsrv in
Router(config-if)#exit
Router(config)#interface fastethernet 0/3
Router(config-if)#mac access-group deny_to_accsrv in
Router(config-if)#end
Router# copy running-config startup-config
```

8.2 网络地址转换

网络地址转换（Network Address Translation，NAT）是将 IP 报头中的源地址或目标地址进行翻译或转换的一种广域网（WAN）技术，主要被用来将内部私有地址转换为公有地址。

NAT 的典型应用是将使用私有 IP 地址的园区网络连接到 Internet 上，这样，公司就无需给内部网络中的每个设备分配公有 IP 地址，既避免了公有地址的浪费，又节省了申请公有 IP 地址的费用，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

8.2.1 NAT 概述

NAT 有几种类型，如网络地址转换和端口地址转换（Port Address Translation，PAT）。由

于使用了许多术语，地址转换的概念容易让人混淆，特别是许多人不能正确地使用地址转换的术语。表 8-1 和表 8-2 分别给出了地址转换中常用的术语和地址转换类型的一些术语。

表 8-1　常用的地址转换术语

术语	定义
内部	位于网络内部的网络
外部	位于网络外部的网络
本地	物理分配给设备的 IP 地址
全局	物理或逻辑分配给设备的公共 IP 地址
内部本地 IP 地址	分配了私有 IP 地址的内部设备
内部全局 IP 地址	分配了公有 IP 地址的内部设备
外部全局 IP 地址	分配了公有 IP 地址的外部设备
外部本地 IP 地址	分配了私有 IP 地址的外部设备

表 8-2　常用的地址转换类型

转换类型	解释
标准	一个 IP 地址转换成一个不同的 IP 地址
扩展	将一个 IP 地址和一个 TCP/UDP 端口号映射成一个不同的 IP 地址，可能包含端口号
静态	在两个地址之间执行手工地址转换，可能包括端口号
动态一个地址	转换设备在两个地址间自动执行地址转换，可能包含端口号
网络地址转换	只转换 IP 地址（不包括端口号）
端口地址转换	把许多内部 IP 地址转换成一个单独的 IP 地址，每一个内部地址通过给定一个不同的端口号来确定转换的唯一性

1. 网络地址转换

网络地址转换把一个 IP 地址转换为另一个 IP 地址，被转换的 IP 地址可以是源地址或目标地址。在 NAT 中，有静态和动态两种基本实现方法。

❑ **静态 NAT**

使用静态 NAT，地址转换设备执行手动转换将一个地址转换为另一个不同的地址。典型情况下，静态 NAT 用来转换进入网络的数据包中的目标 IP 地址，但也可用来转换源地址。

图 8-5 给出了一个外部用户访问内部 Web 服务器的简单实例。在该实例中，希望 Internet 上的用户访问内部的 Web 服务器，但该服务器使用了私有地址（10.1.1.1）。这样，如果外部用户将私有地址放入目标 IP 地址字段中，他们的 ISP 将会丢弃该数据包。因此，Web 服务器需要具有一个公共地址（这是在地址转换设备中定义的）。

Web 服务器分配一个内部全局 IP 地址 200.200.200.1，在路由器和 DNS 服务器上将该地址通告给外部用户。当外部用户向 200.200.200.1 地址发送数据时，路由器会检查它的转换表寻找匹配条目。在该实例中，会发现 200.200.200.1 映射成 10.1.1.1。随后路由器将目标 IP 地址更改为 10.1.1.1，并将数据包转发到内部 Web 服务器。注意如果路由器不转换成 10.1.1.1，由于外部用户最初是将流量发送到 200.200.200.1，Web 服务器是不会知道这个信息是给它自己的。同样，当 Web 服务器发送流量到外部公共网络时，路由器会比较转换表中的源地址项，

如果发现匹配条目，会将内部本地地址（私有源地址 10.1.1.1）更改为内部全局 IP 地址（公共源地址 200.200.200.1）。

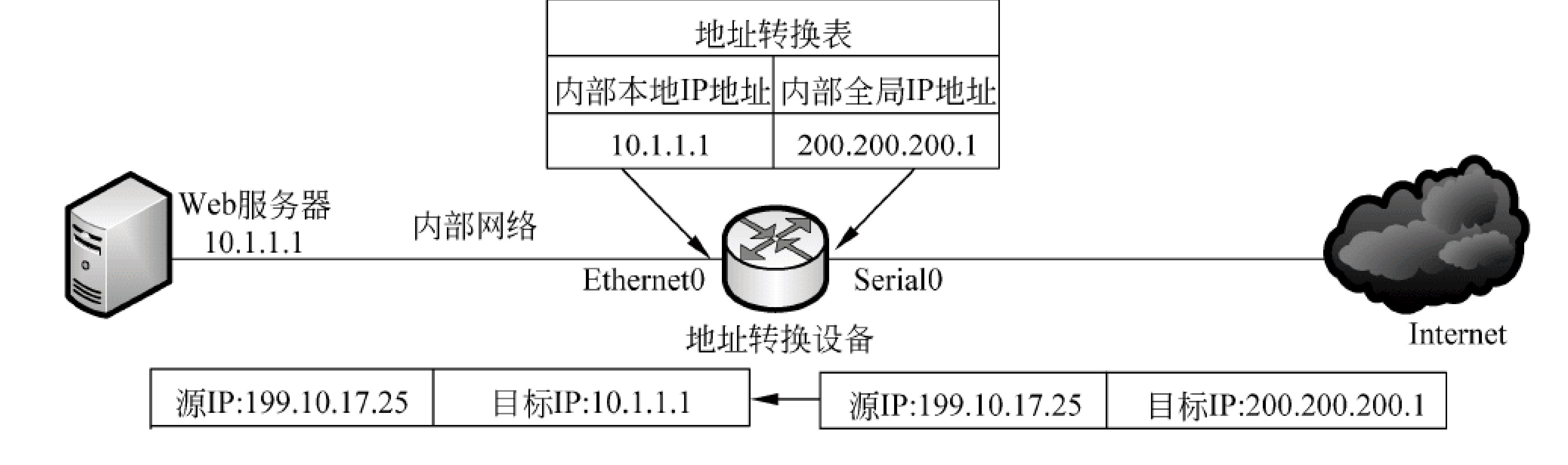


图 8-5　静态地址转换实例

❑ **动态 NAT**

由于使用静态 NAT 时，需要手动建立转换。如果有 1000 台设备，就需要在地址转换表中创建 1000 条静态条目，这将是十分繁重的工作。通常，静态转换是为外部用户需要访问内部资源时服务的，当内部用户访问外部资源时，通常使用动态 NAT。在这种情形下，由于外部设备不需要直接访问内部用户，只需内部用户请求的流量返回给他们，因此分配给内部用户什么地址就不是很重要。

使用动态 NAT，必须在地址转换设备上手动定义两个地址集。一个地址集定义允许转换哪些内部地址，另一个地址集定义这些地址被转换成什么。当内部用户通过地址转换设备（如路由器）发送流量时，该转换设备会检查源地址并将其与内部本地地址池进行比较。如果发现某条目匹配，它会确定哪个内部全局地址池将用来进行转换。随后，它从全局地址池中动态选择一个当前没有分配给内部设备的地址。路由器将该条目加入到地址转换表，并将数据包发送到外部。如果在本地地址池中没有发现匹配条目，地址不会转换，也不会以原始状态转发到外部。

当返回流量回到网络时，地址转换设备会检查目标 IP 地址，并将它们与地址转换表进行比较。当发现匹配条目时，它会将数据包中的目标 IP 地址字段，从全局内部地址转换成本地地址，并将数据转发到内部网络。

2. 端口地址转换

静态或动态 NAT，都只能提供一对一的地址转换。所以，如果有 5000 台具有私有地址的内部设备，并且所有 5000 台设备试图同时访问 Internet，这样在内部全局地址池中就需要 5000 个公有地址。但如果仅有 1000 个公共地址，则只能将前 1000 台设备被转换，剩余 4000 台设备将无法到达外部目的地。

为了解决该问题，可使用成为地址复用（address overloading）的过程。在该过程中，又通常利用端口地址转换和网络地址端口转换（Network Address Port Translation，NAPT）。

利用 PAT，所有通过地址转换设备的计算机都将拥有了分配给它们的相同 IP 地址，因此源端口号用来区分不同的连接。如果两台设备具有相同的源端口号，转换设备将更改其中的一个来确定唯一性。在查看地址转换表时，会显示以下内容。

- ❑ 内部本地 IP 地址（起始源私有地址）。
- ❑ 内部本地端口号（起始源端口号）。
- ❑ 内部全局 IP 地址（被转换的公共源 IP）。
- ❑ 内部全局端口号（新源端口号）。
- ❑ 外部全局 IP 地址（目的公共地址）。
- ❑ 外部全局端口号（目的端口号）。

NAT 与 PAT 相比较，其中一个主要优点是 NAT 基本上可使用大部分 IP 连接类型。由于 PAT 依靠端口号来区分连接，因此 PAT 只能和 TCP/UDP 协议一起工作。

8.2.2 静态地址转换的实现

通常在外部网络设备需要访问如 Web、DNS 和邮件服务器等内部资源时使用静态地址转换。它的实现主要通过在地址转换设备上手动将转换地址和被转换地址一对一映射进行配置。在 IOS 中，必须执行两个基本配置步骤。

- ❑ 定义地址转换类型（全局配置模式命令）。
- ❑ 定义设备位置（端口配置模式命令）。

下面为定义静态地址转换的两条命令。

```
Router(config)#ip nat inside source static inside_local_source_IP_address
inside_global_source_IP_address
Router(config)#ip nat outside source static outside_global_destination_
IP_address outside_local_source_IP_address
```

inside 与 outside 参数指定了转换进行的方向。如 inside 字段指定内部源 IP 地址转换为内部全局 IP 地址；outside 字段将外部目标全局 IP 地址转换为外部本地地址。

配置完成后，需要指定路由器上哪些端口在外部，哪些端口在内部。这可以通过下面配置实现。

```
Router(config)#interface type slot_# / Port_#
Router(config-if)#ip nat inside|outside
```

在连接到内部网络的端口上指定 inside。用图 8-6 所示的网络来进行简单的静态 NAT 配置，在该例中，将为一台内部 Web 服务器（192.168.1.1）分配一个全局 IP 地址（200.200.200.1）。

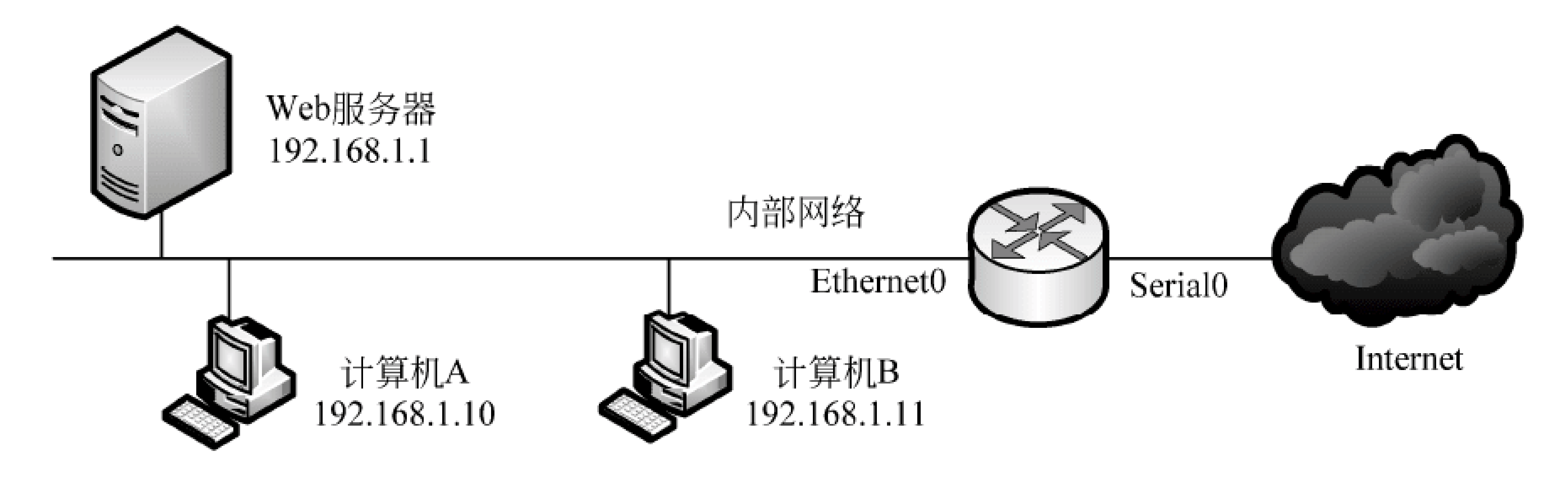


图 8-6　网络地址转换实例

要实现该需求，在路由器上可做如下配置。

```
Router(config)#ip nat inside source static 192.168.1.1 200.200.200.1
Router(config)#interface ethernet 0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router# copy running-config startup-config
```

在该配置列表中，ip nat inside source static 命令定义了转换。ip nat inside 或 outside 命令指定哪个端口在内部（Ethernet 0），哪个端口在外部（Serial 0）。注意，任何不匹配地址转换规则的数据包在通过这两个端口时不会被转换。

8.2.3　动态地址转换的实现

当配置动态 NAT 时，需要配置哪些内部地址被转换、哪些动态地址用于动态转换及哪些端口包括在转换中 3 个部分。要指定转换哪些内部设备的源地址，使用下列命令。

```
Router(config)#ip nat inside source list standard_IP_ACL_# Pool NAT_pool_name
```

ip nat inside source list 命令需要配置一个标准 IP 访问控制列表，来指定用于转换的内部源地址，将转换的任何用 permit 语句列出的地址，不转换任何使用全局源 IP 地址的地址池绑定在一起。

并创建源地址名称来引用从命令 ip nat inside source list 转换而来的内部地址。然后，列出地址池中开始、结束地址及子网掩码。

一旦完成这些，最后需要配置的是哪些端口属于网络的内部端口和外部端口。在此，仍使用图 8-6 所示网络来说明如何配置动态 NAT，但需要在两台计算机上执行动态 NAT，配置列表如下。

```
Router(config)#ip nat inside source list 1 pool nat-pool
Router(config)#access-list 1 permit 192.168.1.10 0.0.0.0
Router(config)#access-list 1 permit 192.168.1.11 0.0.0.0
Router(config)#ip nat pool nat-pool 200.200.200.2 200.200.200.3 netmask
255.255.255.0
Router(config)#interface ethernet 0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router# copy running-config startup-config
```

ip nat inside list 命令指定将要转换内部源地址。注意这些是 ACL 1 中的地址（192.168.1.10

和 192.168.1.11）。它们与成为 nat-pool 的全局地址池关联。ip nat pool 命令指定内部源地址将被转换的全局地址。另外，指定 Ethernet 0 端口为内部，Serial 0 端口指定在外部。

8.2.4 端口复用地址转换

实现端口地址转换时，其配置与配置动态 NAT 非常相似，同样需要 3 条基本转换命令。首先，要指定哪台内部设备将转换其源地址，这里将使用动态 NAT 中用过的相同命令，但要加上 overload 参数指定执行端口复用地址转换。

```
Router(config)#ip nat inside source list standard_IP_ACL_# Pool NAT_pool_name
overload
```

然后，指定使用的全局地址池，其配置命令如下所述。

```
Router(config)#ip nat pool NAT_pool_name Beginning_inside_global_IP_address
ending_inside_global_IP_address netmask subnet_mask_of_address
```

在 PAT 中，可以指定多于一个地址，或指定一个单独的 IP 地址（起始与结束使用相同地址）。最后，必须分别用 ip nat inside 和 ip nat outside 命令通告路由器的哪些端口在内部，哪些端口在外部。

在此，利用图 8-6 所示网络来说明如何配置端口复用地址转换。在该实例中，地址池只有一个单独的 IP 地址（200.200.200.2）。

```
Router(config)#ip nat inside source list 1 pool nat-pool overload
Router(config)#access-list 1 permit 192.168.1.10 0.0.0.0
Router(config)#access-list 1 permit 192.168.1.11 0.0.0.0
Router(config)#ip nat pool nat_pool 200.200.200.2 200.200.200.2 netmask
255.255.255.0
Router(config)#interface ethernet 0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router# copy running-config startup-config
```

8.2.5 网管心得——路由器安全漫谈

较优的路由器本身会采取一个相对完善的安全机制来保护自己，但仅有这一点是远远不够的。保护路由器安全还需要网管员在配置和管理路由器过程中采取相应的安全措施。

1. 堵住安全漏洞

限制系统物理访问是确保路由器安全的最有效方法之一。限制系统物理访问的一种方法

就是将控制台和终端会话配置成在较短闲置时间后自动退出系统。另外，避免将调制解调器（Modem）连接到路由器的辅助端口（AUI 端口）也很重要。

一旦限制了路由器的物理访问，用户一定要确保路由器的安全补丁是最新的。漏洞常常是在供应商（ISP）发行补丁之前被暴露，使得黑客会在供应商发行补丁之前利用受影响的系统，这需要引起用户的关注。

2. 避免身份危机

黑客常常利用弱口令或默认口令进行攻击。加长口令、选用 30 到 60 天的口令有效期等措施有助于防止这类漏洞。如一旦重要的 IT 员工辞职，用户应该立即更换口令，还应该启用路由器上的口令加密功能，这样即使黑客能够浏览系统的配置文件，仍然需要破译密文口令。

另外，实施合理的验证控制也可使路由器安全地传输证书。在大多数路由器上，用户可以配置一些协议，如远程验证拨入用户服务，这样能够使用这些协议结合验证服务器提供经过加密、验证的路由器访问。验证控制可将用户的验证请求转发给通常在后端网络上的验证服务器，还可以要求用户使用双因素验证，以此加强验证系统。双因素的前者是软件或硬件的令牌生成部分，后者则是用户身份和令牌通行码。其他验证解决方案涉及在安全外壳（SSH）或 IPSec 内传送安全证书。

3. 禁用不必要服务

拥有众多路由服务是件好事，但近来许多安全事件都突显了禁用不需要本地服务的重要性。需要注意的是，禁用路由器上的 CDP 可能会影响路由器的性能；另一个需要用户考虑的因素是定时，它对有效操作网络是必不可少的。即使用户确保了部署期间时间同步，经过一段时间后，时钟仍有可能逐渐失去同步。此时，可利用网络时间协议（NTP）服务，对照有效准确的时间源，以确保网络上的设备时针同步。

不过，确保网络设备时钟同步的最佳方式不是通过路由器，而是在防火墙保护的非军事区（DMZ）区域内放一台 NTP 服务器，将该服务器配置为仅允许向外面的可信公共时间源提出时间请求。在路由器上，用户很少需要运行其他服务（如 SNMP、DHCP），只有绝对必要时才使用这些服务。

4. 限制逻辑访问

限制逻辑访问主要借助于合理处置访问控制列表。限制远程终端会话有助于防止黑客获得系统逻辑访问，但如果无法避免 Telnet，还可使用终端访问控制，以限制只能访问可信计算机。因此，用户需要给 Telnet 在路由器上使用的虚拟终端端口添加一份访问列表。

ICMP 有助于排除故障，但也为攻击者提供了用来浏览网络设备、确定本地时间戳和网络掩码以及对 IOS 修正版本作出推测的信息。为了防止黑客搜集上述信息，只允许以下类型的 ICMP 流量进入用户网络：ICMP 网无法到达的、主机无法到达的、端口无法到达的、包太大的、源抑制的以及超出生存时间（TTL）的。此外，逻辑访问控制还应禁止 ICMP 流量以外的所有流量。

使用入站访问控制将特定服务引导至对应的服务器。例如，只允许 SMTP 流量进入邮件服务器；DNS 流量进入 DNS 服务器；通过安全套接协议层（SSL）的 HTTP（HTTP/S）流量

进入 Web 服务器。为了避免路由器成为 DoS 攻击目标，用户应该拒绝以下流量进入：没有 IP 地址的包、采用本地计算机地址、广播地址、多播地址以及任何假冒的内部地址的包。虽然用户无法杜绝 DoS 攻击，但用户可以限制 DoS 的危害。用户可以采取增加 SYN ACK 队列长度、缩短 ACK 超时等措施来保护路由器免受 TCP SYN 攻击。

用户还可以利用出站访问控制限制来自网络内部的流量。这种控制可以防止内部计算机发送 ICMP 流量，只允许有效的源地址包离开网络。这有助于防止 IP 地址欺骗，减小黑客利用用户系统攻击另一站点的可能性。

5. 监控配置更改

用户在对路由器配置进行修改后，需要对其进行监控。如果用户使用 SNMP，那么一定要选择功能强大的共用字符串，最好是使用提供消息加密功能的 SNMP。如果不通过 SNMP 管理对设备进行远程配置，则最好将 SNMP 设备配置成只读。拒绝对这些设备进行写访问，用户就能防止黑客改动或关闭接口。此外，用户还需将系统日志消息从路由器发送至指定服务器。

为进一步确保安全管理，用户可以使用 SSH 等加密机制，利用 SSH 与路由器建立加密的远程会话。为了加强保护，用户还应该限制 SSH 会话协商，只允许会话用于同用户经常使用的几个可信系统进行通信。

配置管理的一个重要部分就是确保网络使用合理的路由协议。避免使用路由信息协议（RIP），RIP 很容易被欺骗而接受不合法的路由更新。用户可以配置边界网关协议（BGP）和开放最短路径优先协议（OSPF）等协议，以便在接受路由更新之前，通过发送口令的 MD5 散列，使用口令验证对方。以上措施有助于确保系统接受的任何路由更新都是正确的。

8.3 网络攻击安全防范

由于网络应用的不断增多，网络安全问题也越来越突出，且计算机网络连接形式的多样性、终端分布的不均匀性、网络的开放性和网络资源的共享性等因素，致使网络容易遭受病毒、黑客、恶意软件和其他不轨行为的攻击。为确保信息的安全与畅通，研究网络的安全与防范措施显得非常重要。

8.3.1 IP 欺骗防范

IP 欺骗技术就是伪造某台计算机的 IP 地址技术。通过 IP 地址的伪造，使得某台计算机能够伪装成另一台计算机，且这台计算机（伪造者）需要具有某种特权或者被另外的计算机（被伪造者）所信任。

IP 欺骗通常要用编写的程序来实现。通过使用 raxSocket 编程，发送带有假冒的源 IP 地址的数据包，来达到自己的目的。另外，目前网络中，也存在大量可发送伪造 IP 地址的工具包，使用它们可以任意指定源 IP 地址，以免留下自己的痕迹。

1. IP 欺骗

IP 欺骗由若干步骤组成。在进行 IP 欺骗前，首先假定目标计算机已经选定；其次，信任模式已被发现，并找到了一个被目标计算机信任的计算机。黑客为了进行 IP 欺骗，进行以下工作：使得被信任的计算机丧失工作能力，同时采样目标计算机发出的 TCP 序列号，猜测出它的数据序列号；然后，伪装成被信任的计算机，并建立起与目标计算机基于地址验证的应用连接。如果成功，黑客可以使用一种简单的命令放置一个系统后门，以进行非授权操作。

❑ **使被信任计算机丧失工作能力**

一旦发现被信任的计算机，为了伪装成它，要使其丧失工作能力。由于攻击者将要代替真正的被信任计算机，所以必须确保真正被信任的计算机不能接收到任何有效的网络数据，否则将会被揭穿。有许多方法可以做到这些，如“TCP SYN 淹没”。

在建立 TCP 连接时第一步由客户端向服务器发送 SYN 请求；通常，服务器将向客户端发送 SYN/ACK 信号（这里客户端是由 IP 地址确定的）。客户端随后向服务器发送 ACK，然后数据传输就可以进行了。然而，TCP 处理模块有一个处理并行 SYN 请求的最上限，它可以看作是存放多条连接的队列长度。其中，连接数目包括了那些三步握手法没有最终完成的连接，也包括了那些已成功完成握手，但还没有被应用程序所调用的连接。如果达到队列的最上限，TCP 将拒绝所有连接请求，直至处理了部分连接链路。因此，这里是有机可乘的。

黑客向被进攻目标的 TCP 端口发送大量 SYN 请求，这些请求的源地址是使用一个合法的但是虚假的 IP 地址（可能使用该合法 IP 地址的计算机没有开机）。而受攻击的计算机却会向该 IP 地址发送响应的，但始终接受不到确认信息。此时，IP 数据包会通知受攻击计算机的 TCP：该目标计算机不可到达，不过 TCP 会认为是一种暂时错误，并继续尝试连接（比如继续对该 IP 地址进行路由，发出 SYN/ACK 数据包等），直至确信无法连接。

这时，已进行了很长时间。需要注意的是，黑客们是不会使用那些正在工作的 IP 地址的，因为这样，真正 IP 持有者会收到 SYN/ACK 响应，而随之发送 RST（Reset The Connection，连接复位）给受攻击主机，从而断开连接。前面所描述的过程可以表示为如下模式。

1 A （B） －－－SYN －－－＞ C
A （B） －－－SYN －－－＞ C
A （B） －－－SYN －－－＞ C
2 B ＜－－－SYN/ACK－－ C
B ＜－－－SYN/ACK－－ C
3 B ＜－－－ RST －－－ C

在时刻 1 时，攻击计算机（B）发送大量的 SYN 请求给受攻击目标（C），使其 TCP 队列充满。在时刻 2 时，受攻击目标（C）向它所相信的 IP 地址（虚假的 IP）作出 SYN/ACK 反应。在这一期间，受攻击主机的 TCP 模块会对所有新的请求予以忽视。不同的 TCP 保持连接队列的长度是有所不同（BSD 一般是 5，Linux 一般是 6）。使被信任主机（A）失去处理新连接的能力，所赢得的空隙时间就是黑客进行攻击目标主机（C）的时间，这使其伪装成被信任主机成为可能。

❑ **序列号取样和猜测**

要对目标进行攻击，必须知道目标计算机使用的数据包序列号。黑客是如何进行预测的

呢？他们首先与被攻击计算机的一个端口（SMTP 是一个很好的选择）建立起正常的连接。通常，这个过程被重复若干次，并将目标计算机最后所发送的初始的序列号（SEQ 标志）ISN 存储起来。

另外，黑客还需要估计目标计算机与被信任计算机之间的 RTT 时间（往返时间），这个 RTT 时间是通过多次统计平均求出的。RTT 对于估计下一个 ISN 是非常重要的。其中，每秒钟 ISN 增加 128000，每次连接增加 64000。这样，就不难估计出 ISN 的大小，它是 128000 乘以 RTT 的一半，如果此时目标计算机刚刚建立过一个连接，那么再加上一个 64000。估计出 ISN 大小后，立即开始进行攻击。当黑客伪造的 TCP 数据包进入目标计算机时，根据估计的准确度不同，将会发生不同的情况。

如果估计的序列号是准确的，进入的数据将被放置在接收缓冲器以供使用。

如果估计的序列号小于期待的数字，那么将被放弃。

如果估计的序列号大于期待的数字，并且在滑动窗口（缓冲）之内，那么该数据被认为是一个未来的数据，TCP 模块将等待其他缺少的数据。如果估计的序列号大于期待的数字，但不在滑动窗口（缓冲）之内，那么 TCP 将会放弃该数据并返回一个期望获得的数据序列号。

2. 防止 IP 欺骗

在典型的 IP 地址欺骗中，攻击者通常伪造数据包的发送地址，以表明自己来自内网。针对这一攻击手段讨论 3 种防范方法。

❑ 阻止 IP 地址

防止 IP 欺骗的一种有效方法是阻止可能造成风险的 IP 地址。不管采用的攻击方式是什么，攻击者可以伪造任何 IP 地址，最常被伪造的 IP 地址是私网 IP 地址和其他类型的共享/特殊 IP 地址，如 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、127.0.0.0/8、224.0.0.0/3 及 169.254.0.0/16 等这些网络 IP 地址。

所有上面这些地址要么是在互联网上不可路由的私网 IP 地址，要么是用作其他用途而根本不应该在互联网上的 IP 地址。如果从互联网上进入的数据包有这些 IP 源地址，那么可判定是骗人的。

❑ 采用访问控制列表（ACLS）

阻止 IP 欺骗的最简单方法是对所有互联网数据进行进站过滤。过滤时将丢弃所有来自 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、127.0.0.0/8、224.0.0.0/3、169.254.0.0/16 这些 IP 地址的数据包。也就是说，通过创建一张访问控制列表，丢弃所有来自上述范围内的 IP 地址的入站数据。这里是一个配置的示例。

```
Router#configure terminal
Router(config)# ip access-list extended ingress-antispoof
Router(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any
Router(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any
Router(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any
Router(config-ext-nacl)# deny ip 127.0.0.0 0.255.255.255 any
Router(config-ext-nacl)# deny ip 224.0.0.0 31.255.255.255 any
Router(config-ext-nacl)# deny ip 169.254.0.0 0.0.255.255 any
```

```
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)#interface fastethernet 1/0
Router(config-if)#ip access-group ingress-antispoof in
Router(config)#end
Router# copy running-config startup-config
```

根据 RFC 2267 规定，互联网服务提供商（ISP）必须在网络上使用类似这一类的过滤。注意末尾处 ACL 包含拒绝所有（permit ip any any）规则。在一些中小型企业中，则可利用一台拥有状态式防火墙（stateful fireful）的路由器，保护内部局域网。

另外，利用创建访问列表方式，还能够过滤所有来自内网中其他子网的进站信息，以便保证局域网子网间进行 IP 地址欺骗，或者实施出站 ACL 来防止本网络中的用户伪造其他网络的 IP 地址。

❑ **使用反向路径转发**

另一个避免 IP 地址欺骗的方法是使用反向路径转发（Reverse Path Forwarding），也称为 IP 验证。在 Cisco IOS 中，反向路径转发的命令以 ip verify 开头。

RPF 的工作原理和反垃圾邮件解决方案非常类似。反垃圾邮件解决方案是收到了邮件消息后，先提出源邮件地址，然后执行向发送服务器查询的操作，确定发送者是否真的在发出消息的服务器上存在。如果发送者不存在，服务器则丢弃该邮件消息，因为根本无法回复这种消息，而且大体上属于垃圾邮件。

RPF 对数据包所作的操作与此类似。它从互联网收到数据包，取出源 IP 地址，然后查看该路由器的路由表中是否有该数据包的路由信息。如果路由表中没有其用于数据返回的路由信息，那么该数据包极有可能是某人伪造的，于是路由便把它丢弃。下面是在路由器配置 RPF 的方法。

```
Router#configure terminal
Router(config)# ip cef
Router(config)# interface serial0/0
Router(config-if)# ip verify unicast reverse-path
Router(config-if)#end
Router# copy running-config startup-config
```

8.3.2　Ping 攻击防范

常用的 Ping 命令，是用来检查网络是否畅通的一个简单且有效的工具。但有时也能给 Windows 系统带来不可预测的灾难（系统崩溃），那就是 Ping 攻击，即所谓的 ICMP 攻击，后果非常严重。

1. Ping 攻击

Ping 攻击，实际上就是通过 Ping 大量的数据包，使得计算机的 CPU 使用率居高不下而崩溃。一般情况下，黑客通常在一个时段内连续向计算机发出大量请求导致 CPU 占用率太高而

死机。基于 Ping 的攻击可以分为两大类，一是 Ping 攻击导致拒绝服务（DoS）；另外一个是基于重定向（redirect）的路由欺骗技术。

其中，拒绝服务攻击是最容易实施的攻击行为。目前，基于 Ping 的攻击绝大部分都可以归类为拒绝服务攻击，其又可以分成针对带宽的 DoS 攻击、针对主机的 DoS 攻击和针对连接的 DoS 攻击 3 种。

❑ **针对带宽的 DoS 攻击**

针对带宽的 DoS 攻击，主要是利用无用的数据来耗尽网络带宽。Pingflood、pong、echok、flushot、fraggle 和 bloop 是常用的 Ping 攻击工具。通过高速发送大量的 ICMP Echo Reply 数据包，目标网络的带宽瞬间就会被耗尽，从而阻止了合法的数据通过网络。由于 ICMP Echo Reply 数据包具有较高的优先级，所以在一般情况下，网络总是允许内部计算机使用 Ping 命令。

这种攻击仅限于攻击网络带宽，单个攻击者就能发起这种攻击。更厉害的攻击形式，如 smurf 和 papa-smurf，可以使整个子网内的计算机对目标计算机进行攻击，从而扩大 ICMP 流量。使用适当的路由过滤规则可以部分防止此类攻击，如果想完全防止这种攻击，就需要使用基于状态检测的防火墙。

❑ **针对主机的 DoS 攻击**

针对主机的 DoS 攻击，主要是攻击操作系统的漏洞。“Ping of Death”及其相关的攻击利用计算机操作系统的漏洞直接对目标计算机发起攻击。

早期路由器对包的最大尺寸都有限制，许多操作系统对 TCP/IP 栈的实现在 ICMP 包上都是规定 64KB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区，当产生畸形的，声称自己的尺寸超过 ICMP 上限的包也就是加载的尺寸超过 64KB 上限时，就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使接收方宕机。

根据这个原理，通过发送一个非法的 ICMP Echo Request 数据包，就能够使目标系统崩溃或重启。许多系统包括 Windows、UNIX、Macintosh，甚至还有一些路由器和打印机，都容易遭受此类攻击。

如果用户使用的操作系统的版本过旧，请确保是否打好了补丁。这类攻击包括 pinger、pingexploit、jolt、jolt2、Sping、Ssping、IceNewk 和 ICMPbug。一个能执行详细数据包完整性检测的防火墙，可以防止所有这种类型的攻击。

❑ **针对连接的 DoS 攻击**

针对连接的 DoS 攻击，可以终止现有的网络连接。针对网络连接的 DoS 攻击会影响所有的 IP 设备，因为它使用了合法的 ICMP 消息。例如，Nuke 攻击通过发送一个伪造的 ICMP Destination Unreachable 或 Redirect 消息来终止合法的网络连接。更具恶意的攻击，如 puke 和 smack，会给某一个范围内的端口发送大量的数据包，毁掉大量的网络连接，同时还会消耗受害计算机 CPU 的时钟周期。

还有一些攻击使用 ICMP Source Quench 消息，导致网络流量变慢，甚至停止。Redirect 和 Router Announcement 消息用来强制受攻击计算机使用一个并不存在的路由器，并把数据包路由到攻击者的计算机进行攻击。针对连接的 DoS 攻击不能通过打补丁的方式加以解决，需要过滤适当的 ICMP 消息类型，一般防火墙可以阻止此类攻击。

❑ **基于重定向的路由欺骗技术**

微软的 Windows Server 2003 和 2008 系统中，都保持着一张已知的路由器列表，位于第

一项的路由器是默认路由器，如果默认路由器关闭，则位于列表第二项的路由器成为默认路由器。默认路由器向发送者报告另一条到特定计算机的更短路由，就是 ICMP 重定向。

攻击者可利用 ICMP 重定向报文破坏路由，以此增强其窃听能力。除了路由器，计算机必须服从 ICMP 重定向。如果一台计算机要向网络中的另一台计算机发送一个 ICMP 重定向消息，这就可能引起其他计算机具有一张无效的路由表。若一台计算机伪装成路由器，截获所有到某些目标网络或全部目标网络的 IP 数据包，这样形成了窃听。

另外，通过 ICMP 技术还可对防火墙后的计算机进行攻击和窃听。

2. Ping 攻击防御

判断是否存在这种攻击的方法只需判断数据包的大小是否大于 65535 字节。反攻击的方法是使用新的补丁程序，当收到大于 65535 字节的数据包时，丢弃该数据包，并进行系统审计。

目前所有的标准 TCP/IP 协议，都具有对付超过 64KB 大小的数据包的能力，且大多数具有防火墙功能的路由器，能够通过对数据包中的信息和时间间隔的分析，自动过滤这些攻击。Windows 98、Windows NT 4.0（SP3 之后）、Windows 2000/XP/Server 2003、Linux 和 Solaris 等系统都已具有抵抗一般的“Ping of death”拒绝服务攻击的能力。此外，对防火墙进行配置，阻断 ICMP 及任何未知协议数据包，都可以防止此类攻击的发生。

8.3.3 DoS 和 DDoS 攻击防范

DoS（Denial of Service 拒绝服务）和 DDoS（Distributed Denial of Service 分布式拒绝服务）攻击是大型网站和网络服务器的安全威胁之一。它们通过占用网络资源，使其他计算机不能进行正常访问，从而导致宕机或网络瘫痪。

在 DoS 和 DDoS 攻击中，主要分为 Smurf、SYN Flood 和 Fraggle3 种。在 Smurf 攻击中，攻击者使用 ICMP 数据包阻塞服务器和其他网络资源；SYN Flood 攻击使用数量巨大的 TCP 半连接来占用网络资源；Fraggle 攻击与 Smurf 攻击原理类似，使用 UDP echo 请求而不是 ICMP echo 请求发起攻击。SYN Flood 由于其攻击效果好，已经成为目前最流行的 DoS 和 DDoS 攻击手段。

SYN Flood 利用 TCP 协议缺陷，发送了大量伪造的 TCP 连接请求，使得被攻击方资源耗尽，无法及时回应或处理正常的服务请求。一个正常的 TCP 连接需要三次握手，首先客户端发送一个包含 SYN 标志的数据包，其后服务器返回一个 SYN/ACK 的应答包，表示客户端的请求被接受，最后客户端再返回一个确认包 ACK，这样才完成 TCP 连接。在服务器端发送应答包后，如果客户端不发出确认，服务器会等待到超时，期间这些半连接状态都保存在一个空间有限的缓存队列中；如果大量的 SYN 包发送到服务器端后，服务器没有作出应答，就会使服务器端的 TCP 资源迅速耗尽，导致正常的连接不能进入，甚至会导致服务器的系统崩溃。

尽管网络安全专家都在着力开发阻止 DoS 和 DDoS 攻击的设备，但收效不大（因为 DoS 和 DDoS 攻击利用了 TCP 协议本身的弱点）。正确配置路由器能够有效防止这些攻击，在此以 Cisco 路由器为例，因为在 Cisco 路由器中的 IOS 软件具有许多防止 DoS 和 DDoS 攻击的特性，保护路由器自身和内部网络的安全。

1. 使用扩展访问列表

扩展访问列表是防止 DoS 和 DDoS 攻击的有效工具，它既可以用来探测 DoS 和 DDoS 攻击的类型，也可阻止这些攻击。Show ip access-list 命令能够显示每个扩展访问列表的匹配数据包，根据数据包的类型，用户就可以确定 DoS 和 DDoS 攻击的种类。

如果网络中，出现了大量建立 TCP 连接的请求，这表明网络受到了 SYN Flood 攻击，此时用户则可以改变访问列表的配置阻止 DoS 和 DDoS 攻击。

2. 使用 QoS

使用服务质量优化（QoS）特征，如加权公平列队（WFQ）、承诺访问速率（CAR）、一般流量整形（GTS）及定制列队（CQ）等，都可以有效阻止 DoS 和 DDoS 攻击。需要注意的是，不同的 QoS 策略对付不同 DoS 和 DDoS 攻击的效果是有差别的。

例如，WFQ 对付 Ping Flood 攻击要比防止 SYN Flood 攻击更有效，这是因为 Ping Flood 通常会在 WFQ 中表现为一个单独的传输列队，而 SYN Flood 攻击中的每一个数据包都会表现为一个单独的数据流。

此外，可以利用 CAR 来限制 ICMP 数据包流量的速度，防止 Smurf 攻击，也可用来限制 SYN 数据包的流量速度，防止 SYN Flood 攻击。使用 QoS 防止 DoS 和 DDoS 攻击，需要用户弄清楚 QoS 以及 DoS 和 DDoS 攻击的原理，这样才能针对不同类型的 DoS 和 DDoS 攻击采取相应的防范措施。

3. 使用单一地址逆向转发

逆向转发（RPF）是路由器的一个输入功能，该功能用来检查路由器接口所接收的每一个数据包。如果路由器接收到一个源 IP 地址为 10.10.10.1 的数据包，但 CEF（Cisco Express Forwarding）路由表中没有为该 IP 地址提供任何路由信息，则路由器将会丢弃该数据包。因此，逆向转发能够阻止 Smurf 攻击和其他基于 IP 地址伪装的攻击。

使用 RPF 功能需要将路由器设置为快速转发模式（CEF switching），并且不能将启用 RPF 功能的接口配置为 CEF 交换。RPF 在防止 IP 地址欺骗方面比访问列表具有优势，首先，它能够动态地接收动态和静态路由表中的变化；其次，RPF 所需要的操作维护较少；最后，RPF 作为一个反欺骗的工具，对路由器本身产生的性能冲击，要比使用访问列表小得多。

4. 使用 TCP 拦截

Cisco 公司在 IOS 11.3 版以后，引入了 TCP 拦截功能，这项功能可以有效防止 SYN Flood 攻击内部计算机。

在 TCP 连接请求到达目标计算机之前，TCP 拦截通过拦截和验证来阻止这种攻击。TCP 拦截可以在拦截和监视两种模式下工作。在拦截模式下，路由器拦截到达的 TCP 同步请求，并代表服务器建立与客户端计算机的连接，如果连接成功，则代表客户端计算机建立了与服务器的连接，并将两个连接进行透明合并。在整个连接过程中，路由器会一直拦截和发送数据包。对于非法的连接请求，路由器提供更为严格的对于半连接的超时限制，以防止自身的资源被 SYN 攻击耗尽。在监视模式下，路由器被动地观察流经路由器的连接请求，如果连接

超过了所配置的建立时间，路由器将会关闭此连接。

在 Cisco 路由器上，开启 TCP 拦截功能需要两个步骤，一是配置扩展访问列表，以确定需要保护的 IP 地址；二是开启 TCP 拦截。配置访问列表是为了定义需要进行 TCP 拦截的源地址和目标地址，保护内部目标计算机或网络。在配置时，用户通常需要将源地址设为 any（任何源），并且指定具体的目标网络或计算机。如果不配置访问列表，路由器将会允许所有的请求经过。

5. 使用基于内容的访问控制

基于内容的访问控制（CBAC）是对 Cisco 传统访问列表的扩展，它基于应用层会话信息，智能化地过滤 TCP/UDP 数据包，防止 DoS 和 DDoS 攻击。

CBCA 通过设置超时时限值和会话门限值，来决定会话的维持时间以及何时删除半连接。对 TCP 而言，半连接是指一个没有完成三次握手过程的会话。而对于 UDP 而言，半连接是指路由器没有检测到返回流量的会话。

CBCA 正是通过监视半连接的数量和产生的频率来防止 SYN Flood 攻击的。每当有不正常的半连接建立或在短时间内出现大量半连接时，用户可以判定是遭受了 SYN Flood 攻击。CBCA 每分钟检测一次已经存在的半连接数量和试图建立连接的频率，当已经存在的半连接数量超过了门限值，路由器则会删除一些半连接，以保证新建立连接的需求，路由器持续删除半连接，直到存在的半连接数量低于另一个门限值；同样当试图建立连接的频率超出门限值，路由器就会采取相同的措施，删除一部分连接请求，并持续到请求连接的数量低于另一个门限值。通过这种连接不断地监视和删除，CBCA 可以有效防止 SYN Flood 和 Fraggle 的攻击。

路由器是企业内部网络的第一道保护屏障，也是黑客攻击的一个重要目标。如果路由器很容易被攻破，那么企业内部网络的安全也就无从谈起，因此在路由器上采取适当的措施，防止各种 DoS 和 DDoS 攻击是非常必要的。需要注意的是，以上介绍的几种方法，对付不同类型的 DoS 和 DDoS 攻击的能力是不同的，对路由器 CPU 和内存等硬件资源的占用也存在很大的差别。所以，在实际环境中，用户需要根据自身情况和路由器的性能来选择适当的方式。

8.3.4 网管心得——路由器的安全设计

为了使路由器将合法信息完整、及时、安全地转发到目的地，许多路由器厂商开始在路由器中添加安全模块，出现了路由器与安全设备融合的趋势。但从本质上讲，增加安全模块的路由器，在路由器功能实现方面与普通路由器没有区别。所不同的是，添加安全模块的路由器可以通过加密、认证等技术手段增强报文的安全性，与专用安全设备进行有效配合，来提高路由器本身的安全性和所管理网段的可用性。

在介绍路由器所采用的安全技术之前，应先来了解一下网络应用环境对路由器提出的安全要求。

- **完整性** 要求路由器在转发报文过程中，保证信息不会遭到偶然或蓄意的添加、删除、修改、重放等破坏。

- ❑ **保密性** 要求路由器保证信息在发送过程中不会被窃听，即使信息被窃听也不能被破译。
- ❑ **可用性** 要求路由器保证系统或系统资源可被授权用户访问并按照需求使用的特性。
- ❑ **可控性** 要求路由器根据需要对转发信息进行安全监控，对可疑的网络信息进行分析、截留或其他处理。
- ❑ **及时性** 要求路由器保证网络信息能够被及时转发，不会因安全处理而使转发时间超出限度。
- ❑ **抗攻击性** 要求路由器具有抵抗网络攻击的能力。

1. 路由器安全技术

为了满足网络应用环境对路由器的安全要求，许多路由器厂商将防火墙、传输加密（VPN）、IDS、防病毒、URL 过滤（访问控制）、HA（高可用性）等技术引入路由器。

❑ 访问控制技术

用户验证是实现用户安全防护的基础技术。路由器上可以采用多种用户接入的控制手段，如 PPP、Web 登录认证、ACL、802.1x 协议等，保护接入用户不受网络攻击，同时能够阻止接入用户攻击其他用户和网络。基于 CA 标准体系的安全认证，将进一步加强访问控制的安全性。

❑ 传输加密技术

IPSec 是路由器常用的数据加密协议。借助该协议，路由器支持建立虚拟专用网（VPN）。IPSec 协议包括 ESP（Encapsulating Security Payload）封装安全负载、AH（Authentication Header）报头验证协议及 IKE（Internet Key Exchange）密钥管理协议等，可以用在公共 IP 网络上确保数据通信的可靠性和完整性，能够保障数据安全穿越公网而没有被侦听。

由于 IPSec 的部署简便，只需安全通道两端的路由器或主机支持 IPSec 协议，几乎不需对网络现有基础设施进行更动。这正是 IPSec 协议能够确保包括远程登录、客户机、服务器、电子邮件、文件传输及 Web 访问等多种应用程序安全的重要原因。

❑ 防火墙防护技术

采用防火墙功能模块的路由器具有报文过滤功能，能够对所有接收和转发的报文进行过滤和检查，检查策略可以通过配置实现更改和管理，还可以利用 NAT/PAT 功能隐藏内网拓扑结构，进一步实现复杂的应用网关（ALG）功能。

另外，有一些路由器可提供基于报文内容的防护。原理是：当报文通过路由器时，防火墙功能模块可以对报文与指定的访问规则进行比较，如果规则允许，报文将接受检查，否则报文直接被丢弃。如果该报文是用于打开一个新的控制或数据连接，防护功能模块将动态修改或创建规则，同时更新状态表以创建与连接相关的报文。返回的报文只有属于一个已经存在的有效连接，才会被允许通过。

❑ 入侵检测技术

在安全架构中，入侵检测（IDS）是一个非常重要的技术，目前有些路由器和高端交换机已经内置 IDS 功能模块。内置入侵检测模块需要路由器具备完善的端口镜像（一对一、多对一）和报文统计支持功能。

❑ **HA（高可用性）**

提高自身的安全性，需要路由器能够支持备份协议（如 VRRP）和具有日志管理功能，使得网络数据具备更高的冗余性和能够获取更多的保障。表 8-3 所示为路由器中安全机制所对应的安全功能特性。

表 8-3 路由器中安全机制所对应的安全特性

安全特性	安全机制
完整性	加密、数字签名、数据完整性
保密性	加密、通信服务填充、路由选择
可用性	认证交换、数字签名、访问控制
可控性	安全事件检测、安全审计跟踪、数据拦截
抗攻击性	安全预防、安全告警、日志记录、安全恢复

2. 七层安全设计

具体来说，人们将依据不断变化的网络安全需要，从以下七个层面来加强路由器的安全设计。

- ❑ **硬件的安全保障** 模块化的硬件结构体系结构。
- ❑ **软件的安全保障** 自主知识产权的操作系统；操作系统拥有高度模块化结构，能够实施进程空间隔离、数据流和控制流空间隔离。
- ❑ **链路层的安全保障** 广域网上采用 PPP 认证和 EAP-TLS；以太网上采用 802.1x、MAC 地址/端口绑定、VLAN 隔离和 EAP-TLS；对流量峰值设置阈值，通过流量限速抵御 DoS 攻击。
- ❑ **网络层和传输层的安全保障** IPSec 协议、AH/ESP/IKE、3DES 等；基于 IP 的报文过滤；对 ICMP 各种类型报文的过滤处理；根据 TCP/UDP 报文头选项进行过滤；网络处理器实现分类和过滤功能，保证线速。
- ❑ **路由安全** OSPF/BGP/RIP2/IS-IS/RSVP/LDP 支持各种认证方式（不认证、明文认证、HMAC-MD5 认证）。
- ❑ **应用层的安全保障** 防火墙模块。
- ❑ **实现管理安全的手段** SSL（安全套接字）保证 Web 和 CLI（命令行界面）管理的安全通道；SSH 替代 Telnet 的明文管理通道；多种用户登录验证方式；命令行分级视图管理；管理访问策略控制（源地址、登录端口、登录时间控制）；支持 SNMPv3。表 8-4 为七层安全设计所对应的路由器安全特性。

表 8-4 七层安全设计及对应的路由器安全特性

安全特性	硬件	系统软件	链路层	网络层	传输层	应用层	网络管理
完整性	不支持	不支持	不支持	支持	支持	支持	支持
保密性	不支持	不支持	支持	支持	支持	支持	支持
可用性	不支持	支持	支持	支持	支持	支持	支持
可控性	不支持	不支持	不支持	支持	支持	支持	支持
抗攻击性	支持	支持	不支持	不支持	支持	支持	支持

3. 安全特性侧重

路由器是一个庞大的家族，核心路由器和边缘分支路由器从结构到技术原理都有很大不同，因此不同级别的路由器的安全侧重点是不同的。

例如，远程分支路由器主要集成较为完善的加密和 VPN 功能，能够在用户端对数据进行加密或者建立 VPN 通道，这样可以保证信息在广域网上安全地传递。而对于在网络中位于核心位置的高端路由器，则需要综合化的安全实现措施，首先路由器需要具备完善的用户接入认证和控制功能；其次，路由器在应用程序过滤、入侵检测等方面不仅应具备更强大的能力，还应该具备支持 IP 报文加密、MPLS（Multi-Protocol Label Switching，多协议标记交换）等技术。可以说，中低端路由器只需在路由软件中增加特性或者通过添加硬件加密卡即可实现安全功能；而高端路由器则需要综合采用多种安全措施。

为了使路由器在经过诸多与安全相关的复杂报文处理之后，处理性能不会下降，还出现了以网络处理器（NP）为核心构建高端路由器的方式。网络处理器能够较好解决高端路由器的业务能力和性能之间矛盾的问题，同时也适应网络安全变化迅速的特征，代表了路由器未来的发展方向之一。

8.4 使用 SDM 配置路由器

简单地说，SDM 是一款基于图形化的路由器配置和管理工具，拥有直观的操作界面和强大的功能，适用于初级网络管理员。即使用户不了解命令行界面（CLI），同样可以通过智能向导帮助客户快速轻松地部署、配置并监控思科路由器，这使得配置工作更加简洁方便。

8.4.1 Cisco SDM 简介

Cisco SDM 是为基于 Cisco IOS Software 的路由器开发的一种直观的 Web 设备管理工具，使客户无须了解命令行界面（CLI）就能快速容易地部署配置和监控 Cisco 系统路由器。许多 Cisco 路由器和 Cisco IOS Software 版本路由器均可支持 Cisco SDM，例如 Cisco 830 系列、Cisco 1700 系列、Cisco 1800 系列、Cisco 2600XM 系列、Cisco 2800 系列、Cisco 3600 系列、Cisco 3700 系列、Cisco 3800 系列以及某些 Cisco 7200 系列和 Cisco 7301 路由器等。其基本特征表现为以下几点。

1. 易用性和内置应用智能

利用 Cisco SDM，用户不但能轻松地在 Cisco 路由器上配置路由、交换、安全和服务质量（QoS）；还能通过性能监控进行主动管理。目前，Cisco SDM 用户可以利用 Cisco SDM GUI（Cisco SDM 用户管理界面）远程配置和监控 Cisco 路由器，而无须使用 Cisco IOS Software CLI。因为 Cisco SDM GUI 能够帮助 Cisco IOS Software 的非专业用户完成日常操作；提供易于使用的智能向导，和自动执行路由器安全管理并通过全面的在线帮助和指导给予用户帮助。

Cisco SDM 智能向导，可指导用户通过系统的配置 LAN、WLAN 和 WAN 接口、防火墙、

入侵防御系统（IPS）和 IP Securtiy（IPSec）VPN 来逐步完成路由器和安全配置工作，且能够以智能方式检测到错误配置并提出修复建议。例如，WAN 接口由 DHCP 定址，则允许动态主机配置协议（DHCP）流量通过防火墙。除帮助用户在 Cisco SDM 中输入正确数据的详细步骤外，嵌入在 Cisco SDM 中的在线帮助还提供了相应的背景信息。用户可能遇到的网络和安全术语及定义包含在在线词汇表中。

对于熟悉 Cisco IOS Software 及其安全特性的网络专家，Cisco SDM 提供了能够快速配置和精确调整路由器安全特性的先进配置工具，以便网络专家先审核 Cisco SDM 生成的命令再提供路由器配置更改方案。

Cisco SDM 帮助管理员利用安全套接层（SSL）和安全配置（SSH v2）协议连接从远程位置配置和监控路由器，这种技术能够通过互联网在用户的浏览器与路由器之间建立安全连接。在分支办公室部署时，可以从公司总部配置和监控 Cisco SDM 型路由器，因而能减少分支办公室对高级网络管理员的需要。

2. 集成式安全配置

在部署新的路由器时，可以利用国际计算机安全协会（ICSA）和 Cisco 技术支持中心（TAC）推荐的最佳实践来使用 Cisco SDM 快速配置 Cisco IOS Software 防火墙。

先进的防火墙向导，允许高、中、低应用程序防火墙设置的一步部署。Cisco SDM 用户可以配置最强的 VPN 默认值并自动执行安全审计。此外，Cisco SDM 用户还可以执行防火墙的一步路由器锁定，并通过一步 VPN 快速部署安全站点到站点连接。Cisco 推荐的与 Cisco SDM 捆绑在一起的 IPS 签名表可以快速部署蠕虫、病毒和协议攻击抵御系统。通过 Cisco SDM 网络准入控制（NAC）向导，可以简单快速地将 NAC 和客户机安全状态管理集成到现有的网络基础架构中。

当调用已经配置好的路由器时，利用 Cisco SDM 用户只需执行一步安全审计，即能通过与一般安全漏洞的对比，评估出路由器配置的优势和弱点。管理员可以精细调整现有的路由器安全配置，更好地满足企业需要。Cisco SDM 还可以用于日常操作，如监控、故障管理和故障排除等。

3. 路由器配置

除安全配置外，Cisco SDM 还能帮助用户执行路由器服务配置，如 LAN 与 WLAN、WLAN 和 WAN 接口配置、动态路由、DHCP 服务器以及 QoS 策略等。

利用 LAN 配置向导，用户能为以太网接口分配 IP 地址和子网掩码；启动或禁用 DHCP 服务器；为 WAN 和互联网接入配置 xDSL、T1/E1、以太网和 ISDN 接口；对于串行连接实施帧中继、点对点协议（PPP）和高级数据链路控制（HDLC）封装。不仅如此，Cisco SDM 还允许配置静态路由和通用动态路由协议，如“开放最短路径优先”（OSPF）、“路由信息协议”（RIPv2）和“增强型内部网关路由选择协议”（EIGRP）。

目前，利用 Cisco SDM 可以轻松地将 QoS 策略应用到任何 WAN 或 VPN 通道接口。QoS 策略向导具有自动执行 QoS 策略的 Cisco 体系结构原则，能够有效区分实时应用（语音或视频）、关键业务应用（结构化查询语言 SQL、Oracle、Citrix、路由协议等）流量及其他网络流量（Web 电子邮件等）。借助 Cisco SDM 中基于网络的应用程序识别（NBAR）监控，用

户能够以可视方式实时检查应用层流量，并不断分析 QoS 策略对各种应用流量的影响。

4. 监控和故障排除

在监控模式下，Cisco SDM 不仅能够以图形方式快速显示重要路由器资源的状态和性能数据（接口状态（正常或不正常）、CPU 和内存使用情况等），还可利用路由器上的集成式路由和安全特性深入诊断 WAN 和 VPN 连接，并及时排除故障。例如，当排除 VPN 连接故障时，Cisco SDM 将检查从 WAN 接口层到 IPSec Crypto Map 层的路由器配置和连接；当测试每个层次的配置和远程对等连接时，Cisco SDM 将提供成功或失败状态、可能的失败原因以及 Cisco TAC（Cisco 技术支持中心）提出的修复建议。

Cisco SDM 监控模式，不但允许用户检查被 Cisco IOS Software 防火墙拒绝的网络访问企图次数，还可以访问防火墙记录。此外，用户还可以监控详细的 VPN 状态信息，如 IPSec 通道加密或解密的包数以及 Easy VPN 客户机连接细节等。

5. 降低维护成本

Cisco SDM 适合那些对设备部署和网络管理成本敏感，但缺少高技能技术人员的企业分支办公室和中小型商业机构。利用 Cisco SDM，企业能够轻松地实施路由器安全和网络配置，同时，Cisco SDM 生成的 Cisco IOS Software 配置已经过 Cisco 技术支持中心（Cisco TAC）批准，它能够通过内置配置检查、专家配置编辑器和有意义的默认值提高网络和安全管理员的生产率。另外，Cisco SDM 特性还能减少配置出错机会，大大提高网络可靠性。

对于建立了大网络的企业，Cisco SDM 能够通过与 Cisco CNS 配置引擎的集成以可扩展的方式部署路由器。Cisco SDM 生成的 Cisco IOS Software 配置可以导入到 Cisco CNS 配置引擎中，然后以“饼干模子（cookie cutter）”方式部署到数千台的 Cisco 路由器中。

8.4.2 实现 SDM 与路由器连接

Cisco SDM 是一款非常优秀的远程连接管理软件，支持多种协议且使用方便，能够用它来连接网络设备进行调试，如图 8-7 所示。

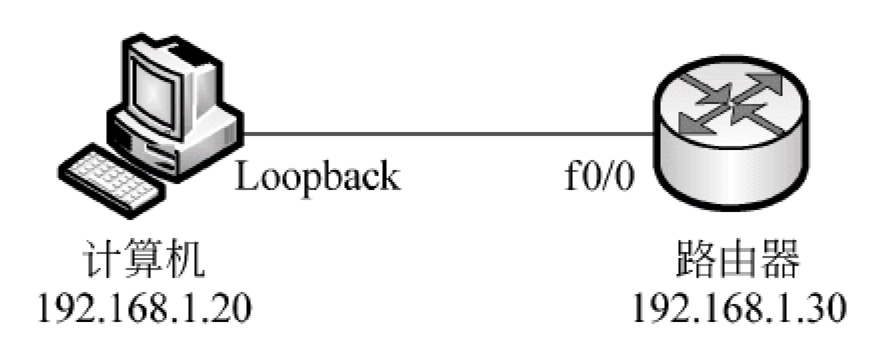


图 8-7　SDM 与路由器连接拓扑图

1. 在计算机上安装 SDM

在安装 SDM 远程管理软件之前，首先要在安装它的计算机上添加 Lookup（回环网卡），如图 8-8 所示，然后设置其 IP 地址为 192.168.1.20。

完成计算机的网卡设置，接着通过双击下载的 SDM 安装程序，启动 Cisco SDM 安装向导，

单击【下一步】按钮，然后在【许可证协议】对话框中，选中【我接受许可证协议中的条款】单选按钮，并单击【下一步】按钮，如图 8-9 所示。




图 8-8 添加 Lookup

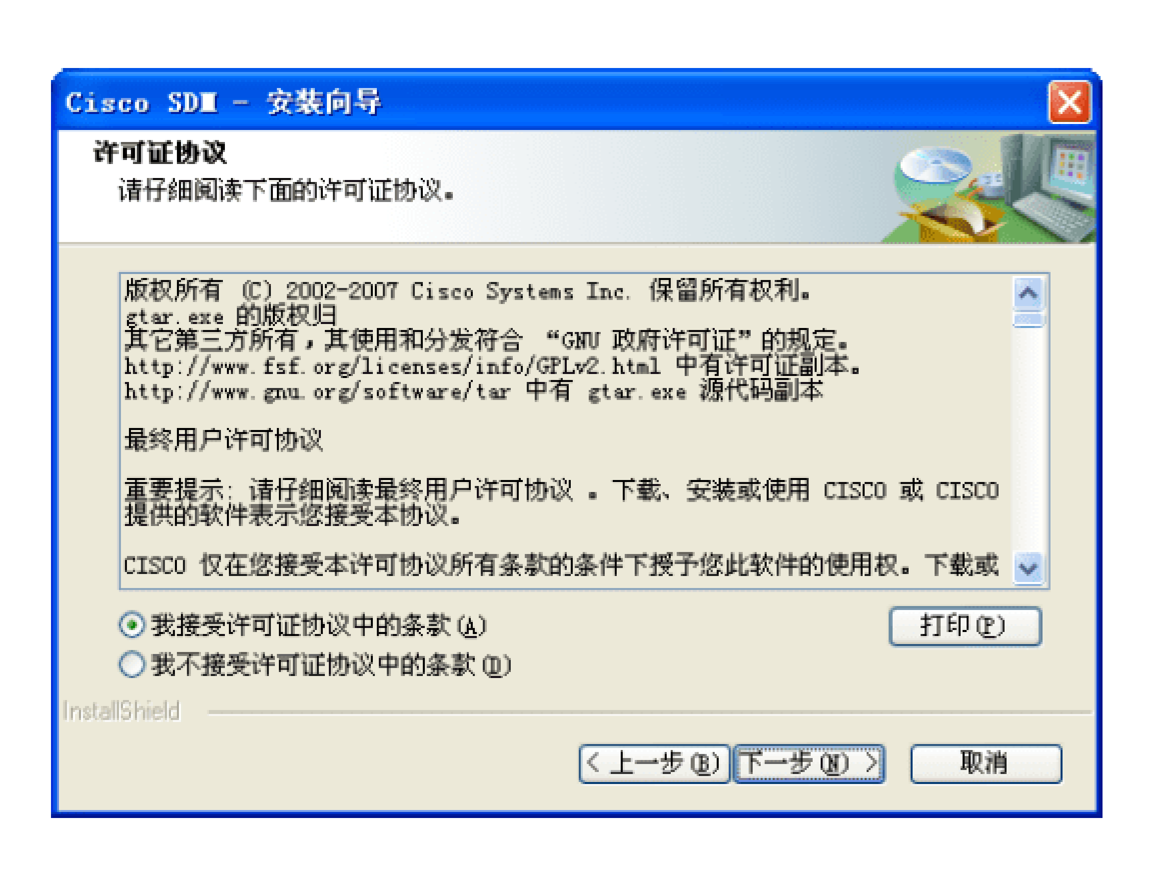
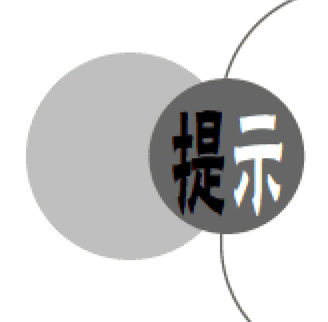


图 8-9 【许可证协议】对话框

这里由于 Cisco SDM 被安装在计算机上，所以在【安装选项】对话框中，选中【本计算机】单选按钮，并单击【下一步】按钮，如图 8-10 所示。



也可以安装到路由器上，大约占用 4MB 的空间，但是会消耗一定的路由器资源，所以，建议用户不要把软件安装到路由器上，而是安装在本地计算机。因为相对来讲，计算机配置比较高，应付这种小软件游刃有余，而路由器的资源让给路由器用比较好。

在【选择目的地位置】对话框中，通过单击【浏览】按钮，设置 SDM 的安装路径为“G:\SDM 安装程序”，并单击【下一步】按钮，如图 8-11 所示。

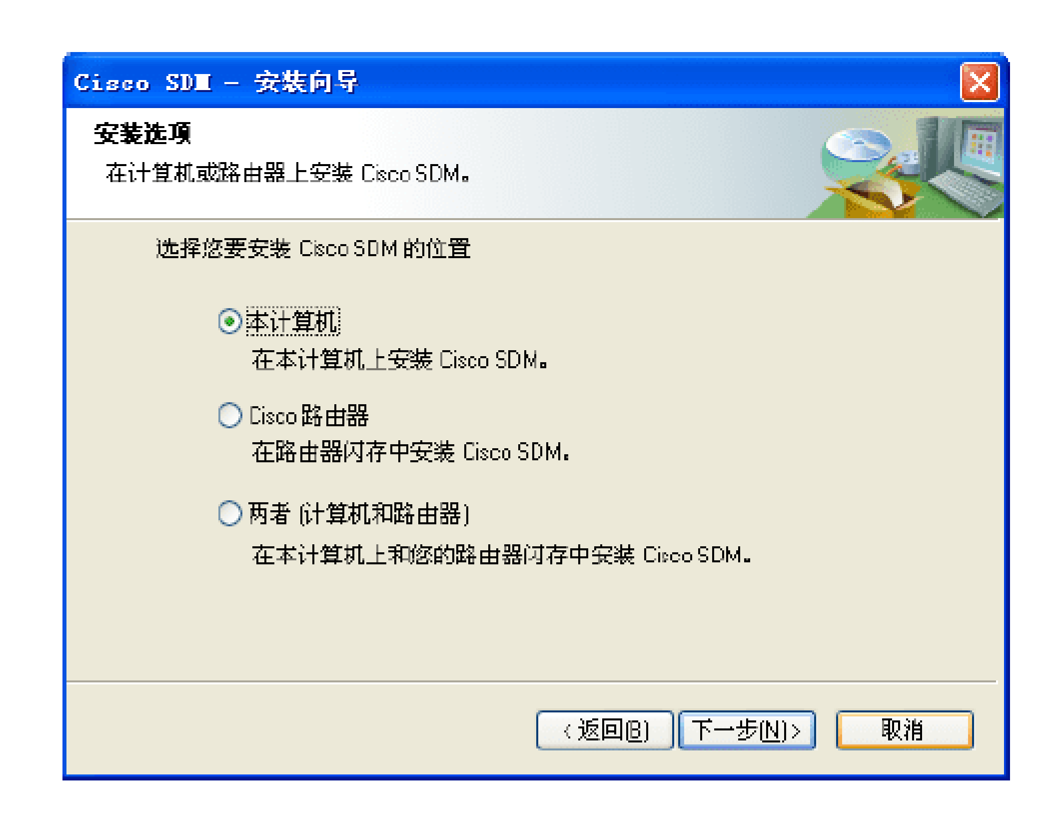


图 8-10 【安装选项】对话框

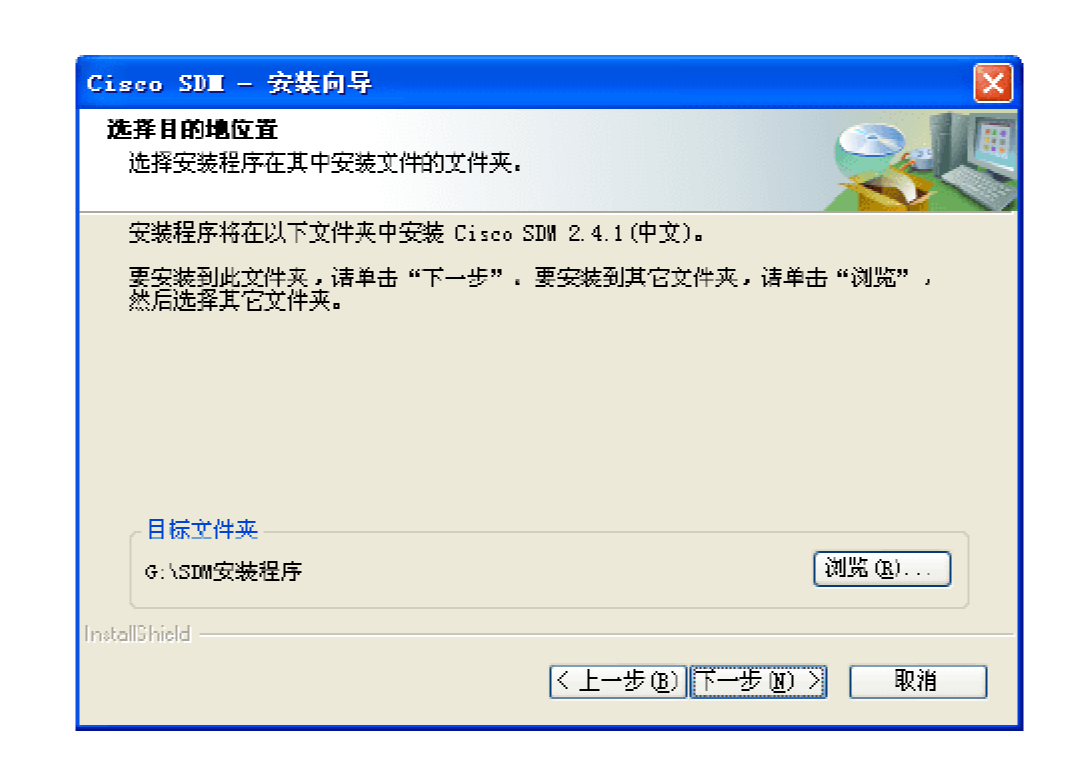


图 8-11 设置 SDM 安装路径

然后，依次在【可以安装该程序了】和【Cisco SDM 安装向导完成】对话框中，单击【安装】和【完成】按钮完成 SDM 的安装。

2．配置路由器，启用 HTTP 服务

SDM 软件成功安装后，还需要在路由器上启用 HTTP 服务，以便在计算机（安装有 SDM 软件）与路由器连接时，使用默认浏览器从该计算机启动 SDM 程序。

若计算机与路由器的 fastethernet 0/0 端口连接，那么需要在路由器的 fastethernet 0/0 端口进行如下配置。

```
Router#configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.30 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip http server
```

到这里，路由器上的配置就完成了。可以在安装 SDM 的计算机上执行【开始】|【程序】|Cisco Systems|Cisco SDM Chinese|Cisco SDM 命令，然后在 SDM Launcher 对话框中输入路由器的 IP 地址 192.168.1.30，并单击【启动】按钮，如图 8-12 所示，来连接路由器。

当 SDM 管理软件与路由器连接成功时，将会在【状态】对话框中提示“当前 SDM 正从您的路由器载入当前配置，请稍候”信息，如图 8-13 所示。



图 8-12　连接路由器

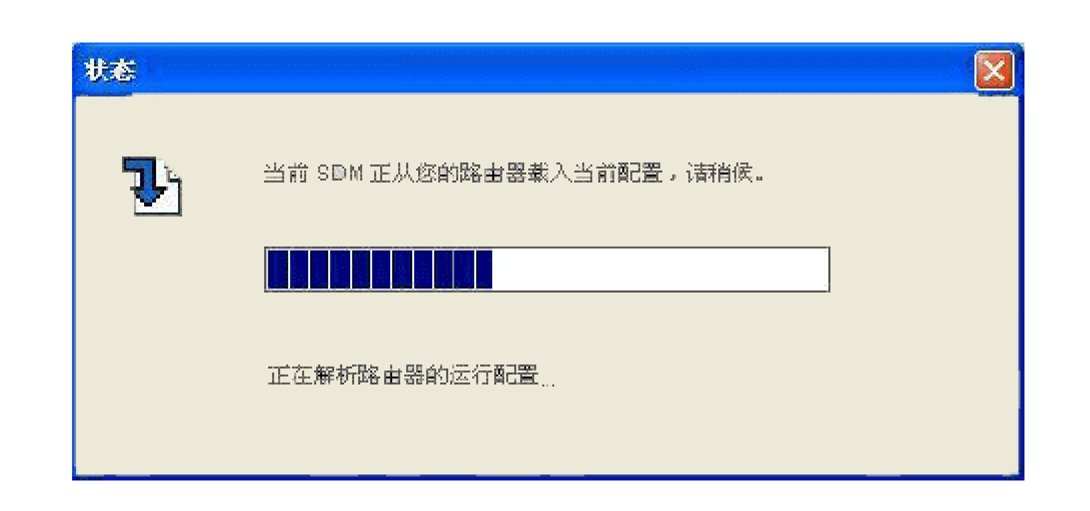


图 8-13 【状态】对话框

8.5　操作实例

8.5.1　操作实例——家庭用路由器安全配置

数据通道和数据控制是路由器的两大典型功能，家庭路由器为用户提供了简单的 Web 管理界面，同时拥有强大的防火墙以及访问控制功能，能够为小型网络提供安全保障。

1．实例目的

- 使用 Web 页面登录路由器。
- 设置防火墙功能。
- 实现 MAC 地址和 URL 过滤。

2. 实例步骤

（1）在桌面执行【开始】|【运行】命令，然后在【运行】对话框中，输入路由器 IP 地址，如“192.168.0.1”，并单击【确定】按钮，如图 8-14 所示。

（2）在弹出的【连接到 192.168.0.1】对话框中，输入用户名和密码，并单击【确定】按钮，如图 8-15 所示。

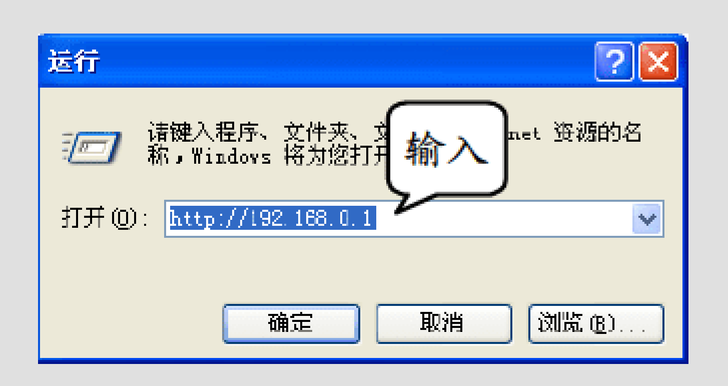


图 8-14 【运行】对话框



图 8-15 输入用户名和密码



图中用户名和密码默认由 ISP 服务商提供给家庭用户。

（3）在【路由器】窗口中，选择【网络安全】选项，如图 8-16 所示。

（4）在【防火墙选项】选项卡内，启用所有复选框，并单击【确定】按钮，如图 8-17 所示。



图 8-16 【路由器】窗口



图 8-17 防火墙选项

（5）选择【MAC 过滤】选项卡，启用【MAC 地址过滤】后的【启用】复选框，单击【MAC 地址】文本框后的下拉按钮，选择 MAC 地址，如“00:14:2A:09:05:DE:/cc01”，然后单击【确定】按钮，如图 8-18 所示。

（6）选择【URL 过滤】选项卡，启用【启用 URL 过滤】复选框，并输入 IP 地址范围，

如“192.168.250-254”，如图 8-19 所示。



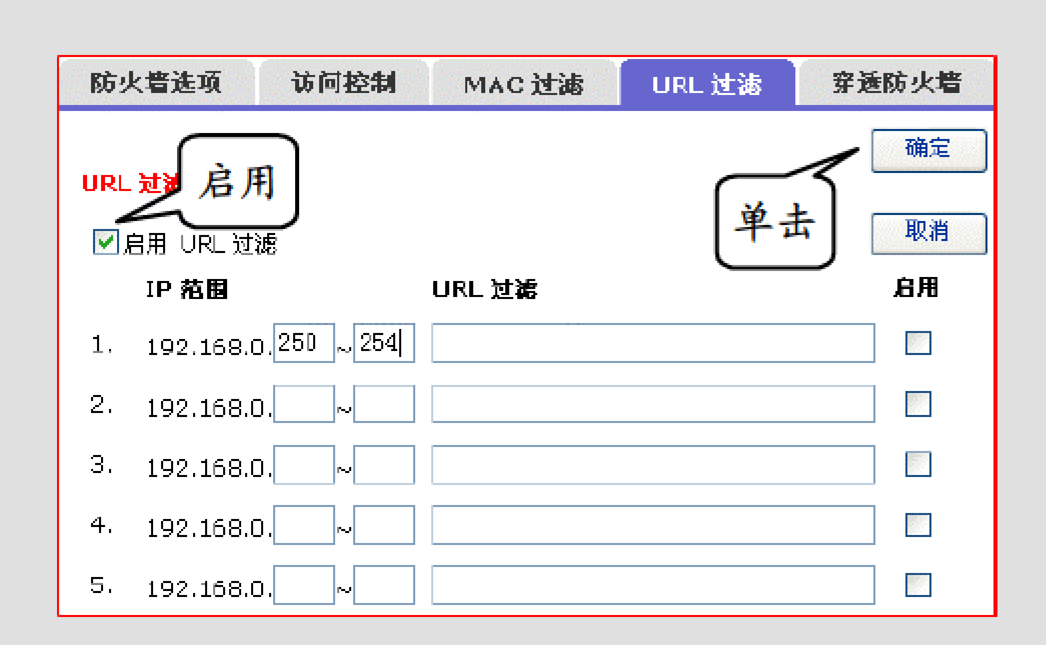
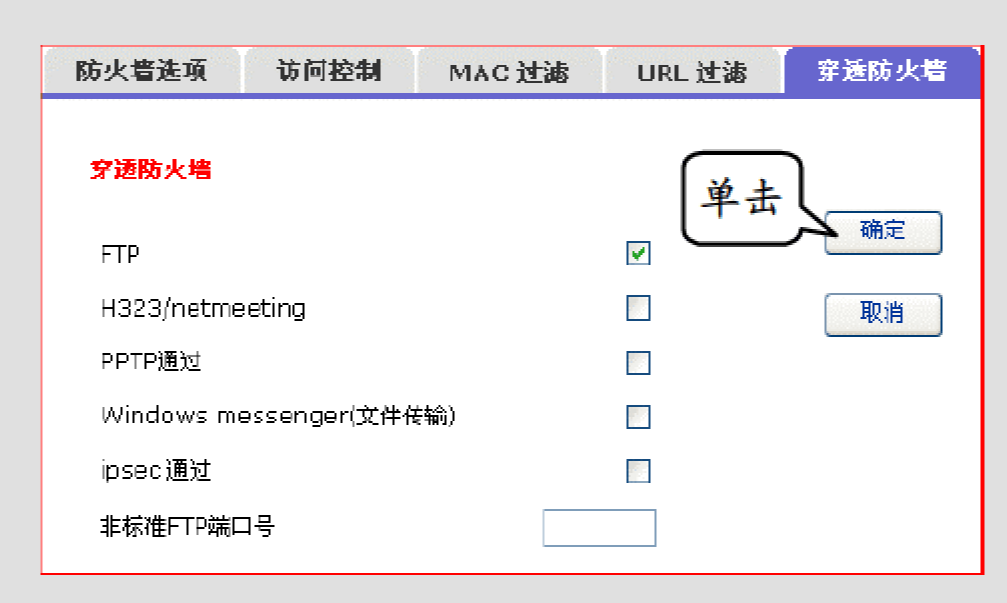


图 8-18　MAC 地址过滤　　　　图 8-19　IP 范围

（7）在【URL 过滤】文本框中，输入 URL 地址，如“www.baidu.com”，并启用文本框后的复选框，然后单击【确定】按钮，如图 8-20 所示。

（8）选择【穿透防火墙】选项卡，启用 FTP 后的复选框，并单击【确定】按钮，如图 8-21 所示。





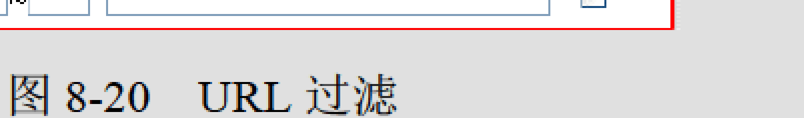


图 8-20　URL 过滤　　　　图 8-21　【穿透防火墙】选项卡

8.5.2　操作实例——为路由器间的协议交换增加认证功能

在路由器上开启 pap 认证，强制通信双方协商用户名和密码，达到相互信任的状态，来保证通信的安全性。

1．实例目的

- ❑ 设置端口 IP 地址。
- ❑ 封装 ppp 协议。
- ❑ 设置认证端与被认证端验证信息。

2．实例步骤

（1）实验拓扑，如图 8-22 所示。

（2）使用图 8-22 所示的在 RA 和 RB 上配置 pap 单向认证功能，RA 的 s1/0 端口与 RB 的 s1/0 端口相连。

（3）在 RA 窗口的 CLI 选项卡中，按回车键，进入用户模式，输入 enable（进入特权模式）命令，并按回车键，如图 8-23 所示。

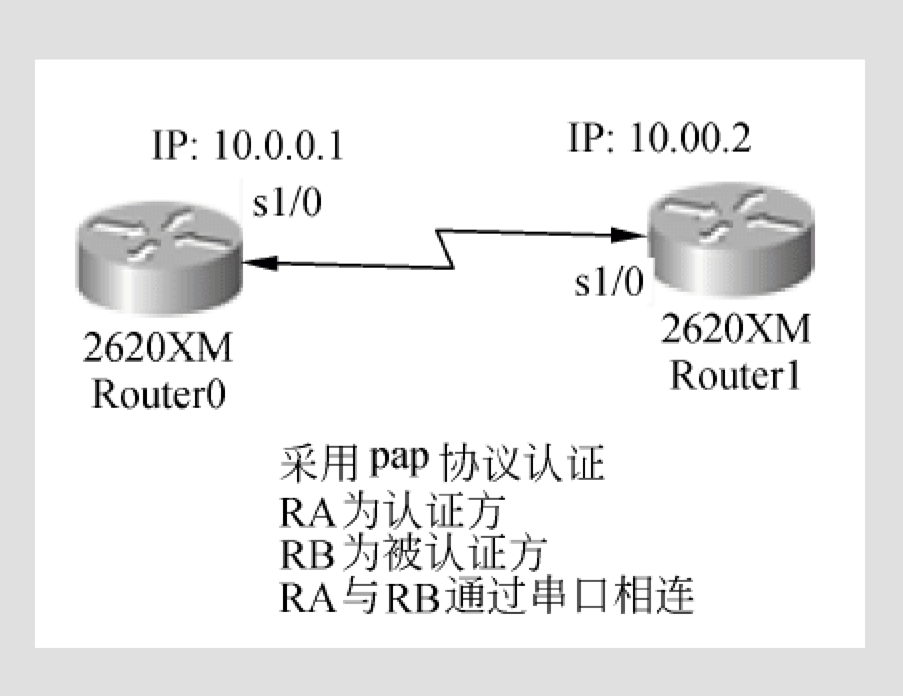


图 8-22　实验拓扑图

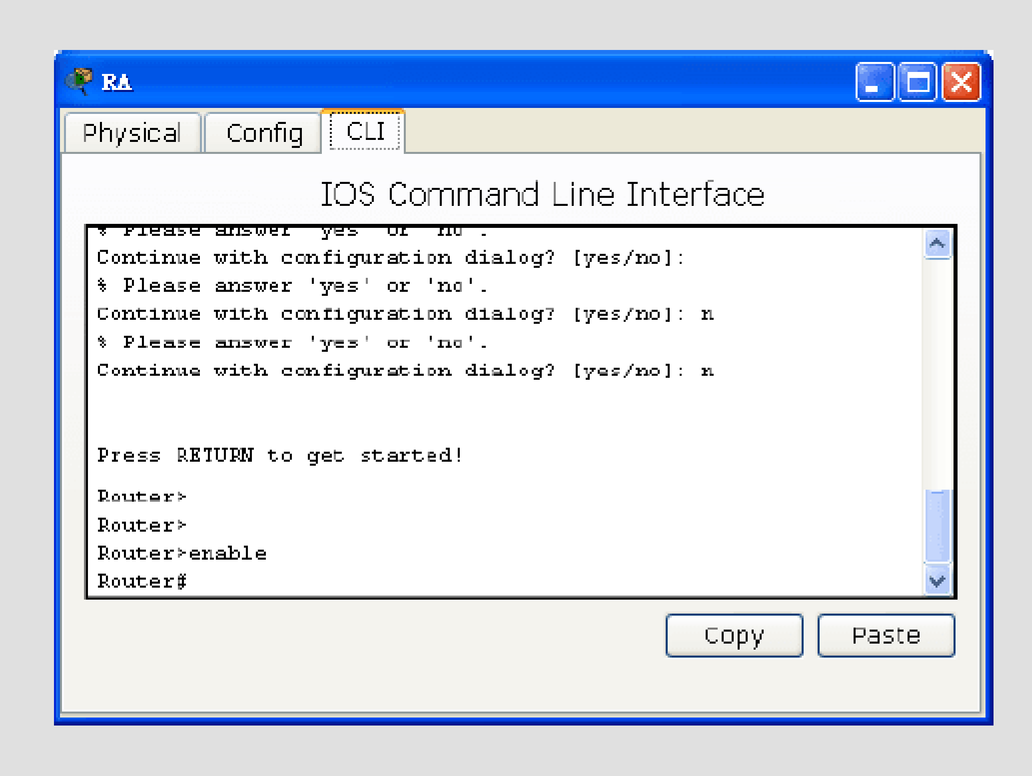


图 8-23　进入特权模式

（4）在特权模式下输入 configure terminal（进入全局模式）命令，并按回车键，如图 8-24 所示。

（5）在全局模式下输入 username cisco password 123456（设置验证信息）命令，并按回车键，如图 8-25 所示。

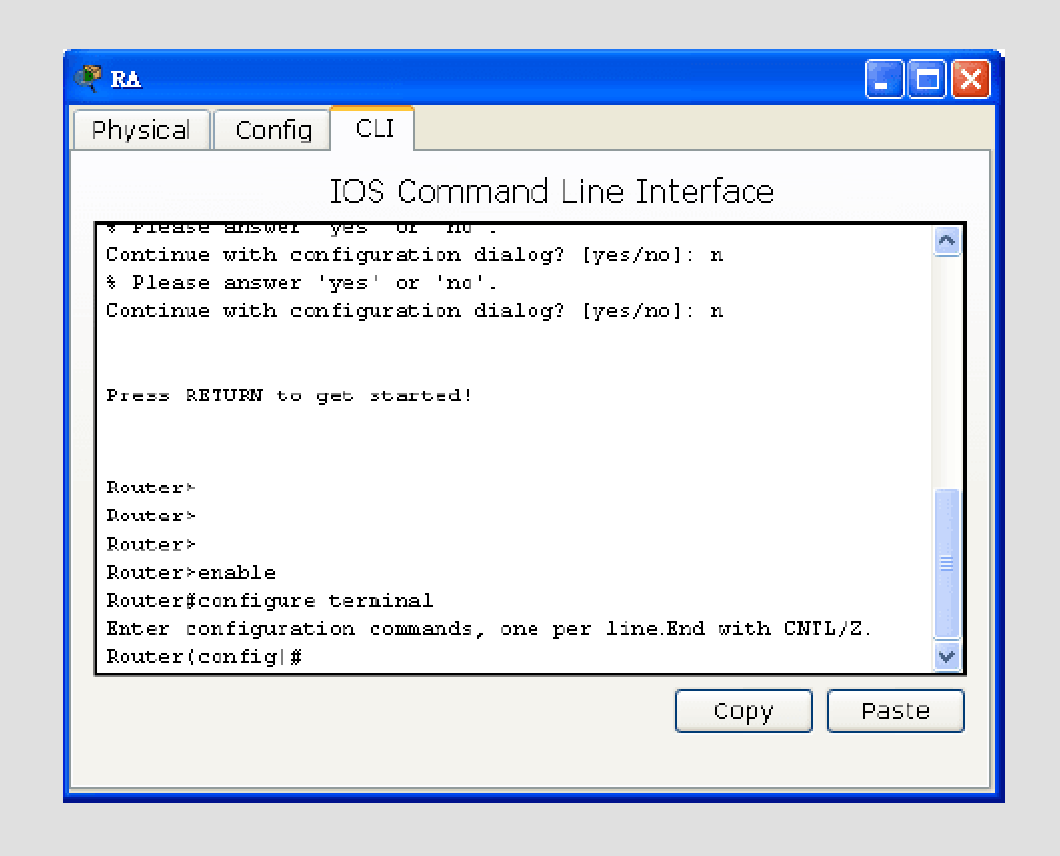


图 8-24　进入全局模式

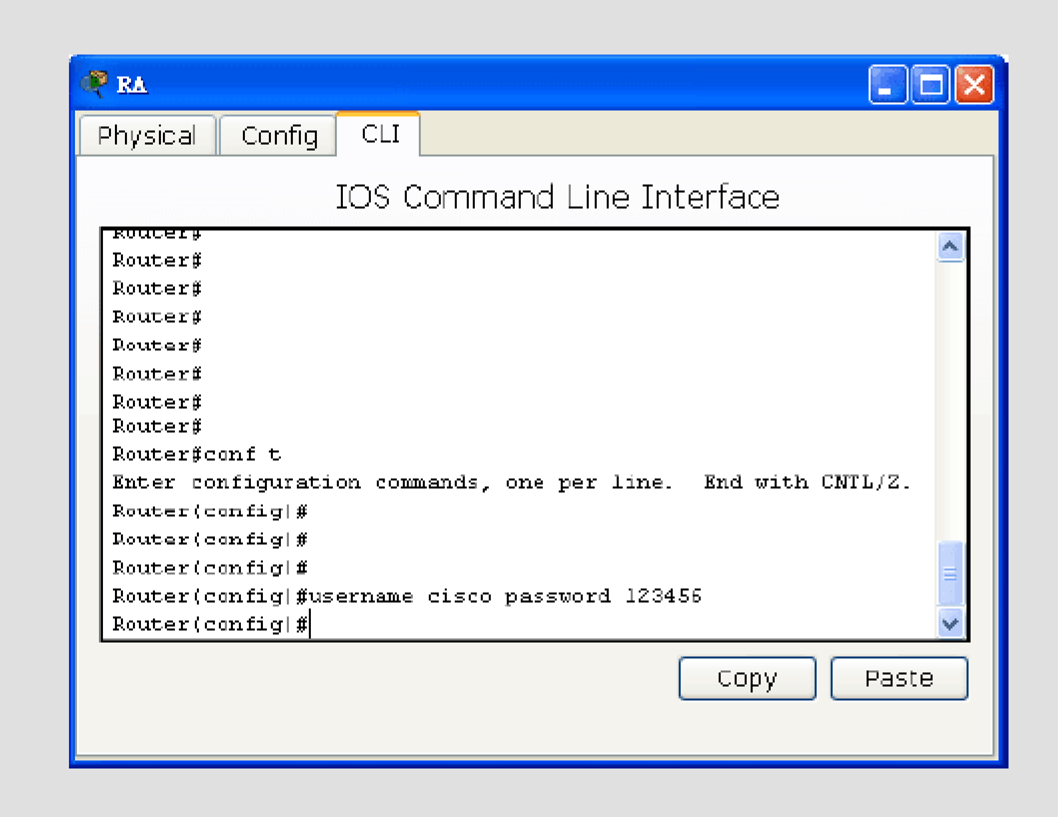


图 8-25　设置验证信息

（6）在全局模式下输入 interface s1/0（进入 s1/0 接口）命令，并按回车键，如图 8-26 所示。

（7）在接口模式下输入 ip address 10.0.0.1 255.0.0.0（为 s1/0 配置 IP 地址）命令，并按回车键，如图 8-27 所示。

（8）在该模式下输入 clock rate 128000（配置端口速率）命令，按回车键，然后输入 no shutdown（开启端口）命令，如图 8-28 所示。

（9）在接口模式下输入 encapsulation ppp（封装 ppp 协议）命令，并按回车键，如图 8-29 所示。

（10）在该模式下输入 ppp authentication pap（开启 pap 认证）命令，并按回车键，如

图 8-30 所示。

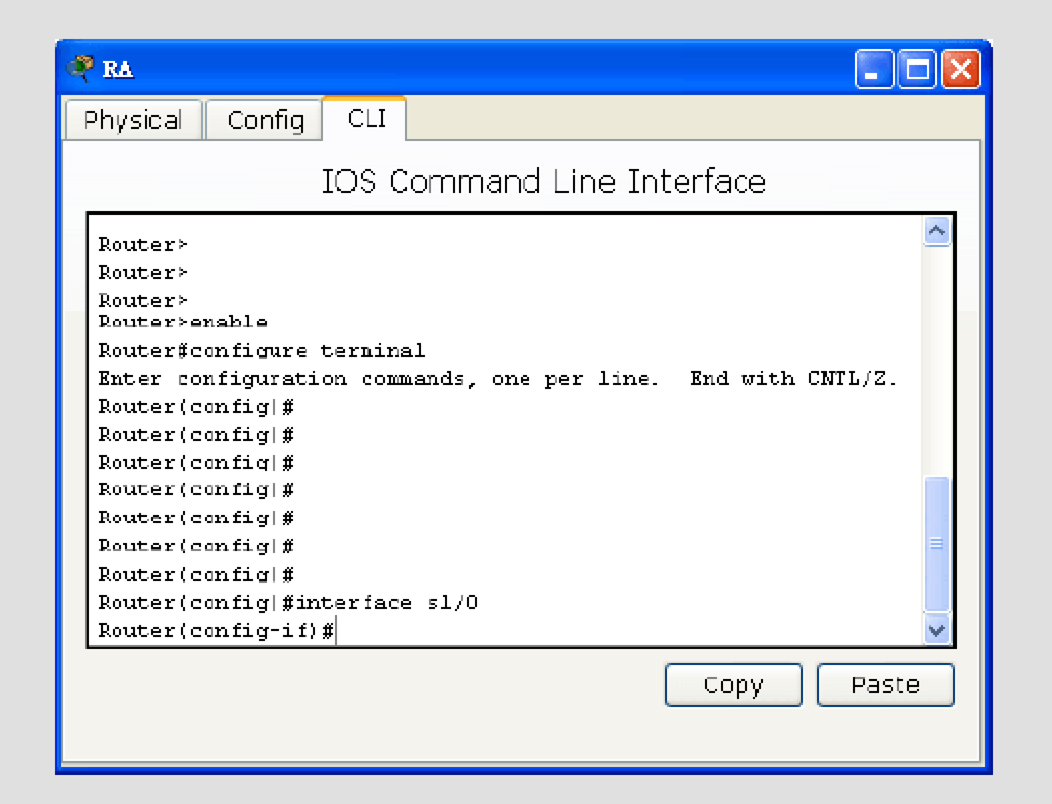


图 8-26　进入 s1/0 接口

图 8-27　配置 s1/0 的 IP 地址

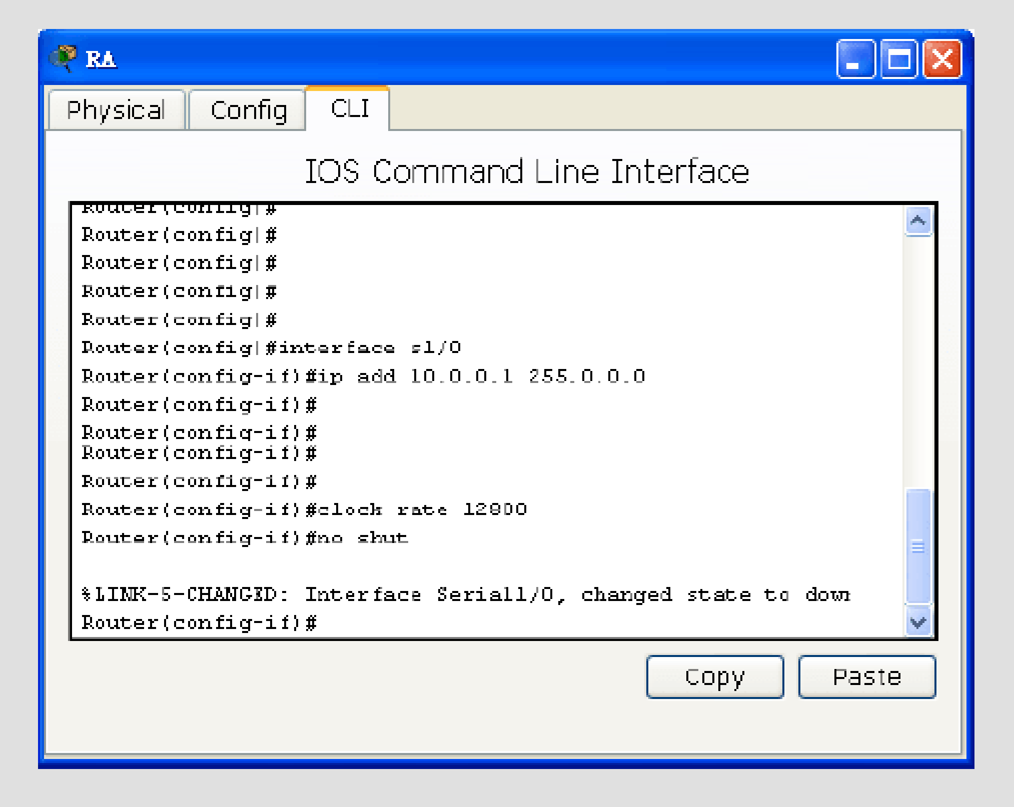


图 8-28　配置端口速率并开启端口

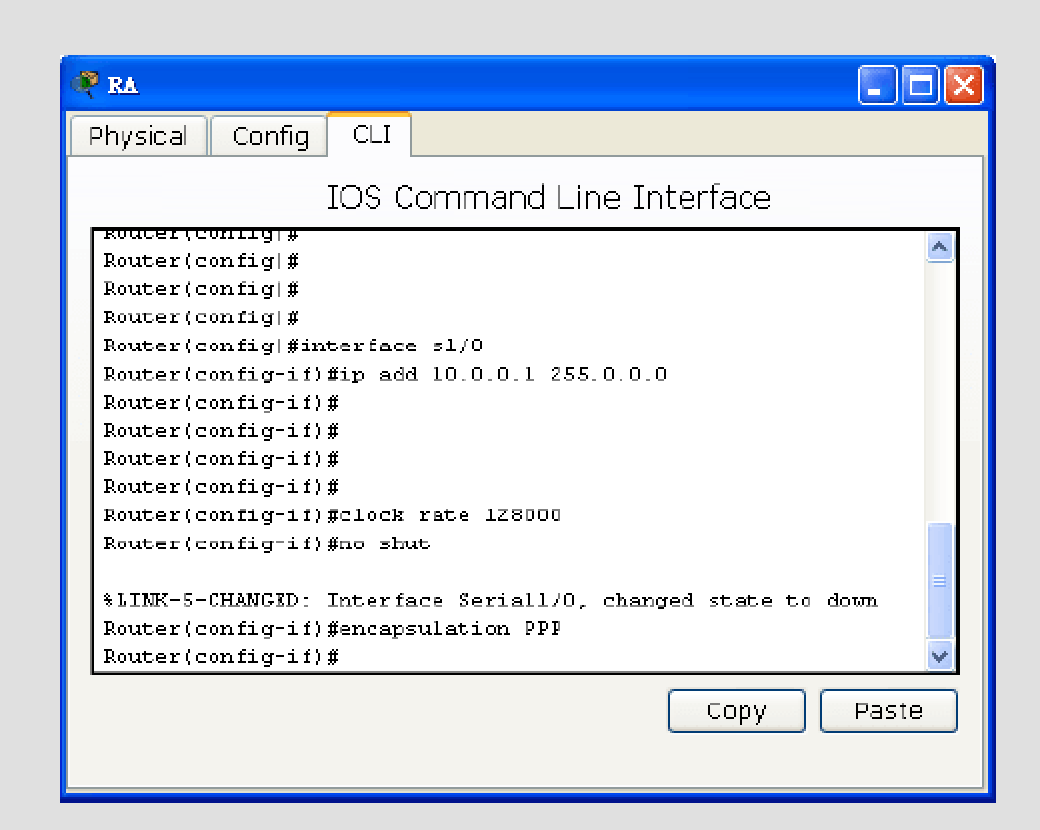


图 8-29　封装 ppp 协议

（11）在 RB 窗口的 CLI 选项卡中，按回车键，输入 enable（进入特权模式）命令，如图 8-31 所示。

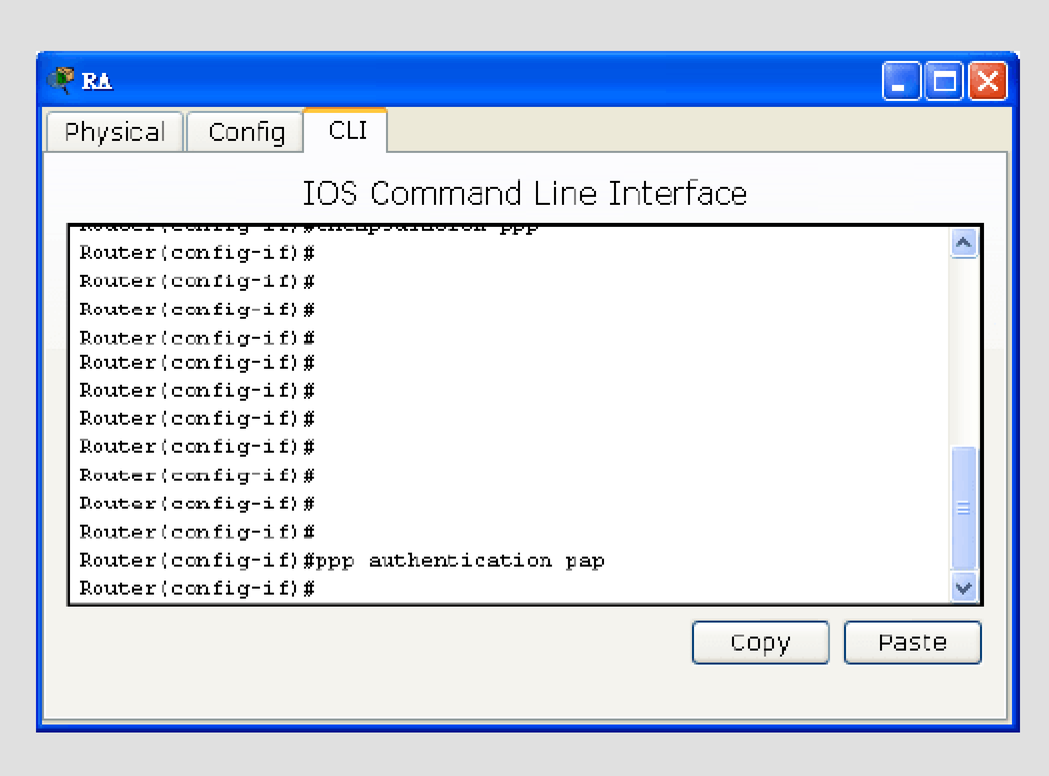


图 8-30　开启 pap 认证

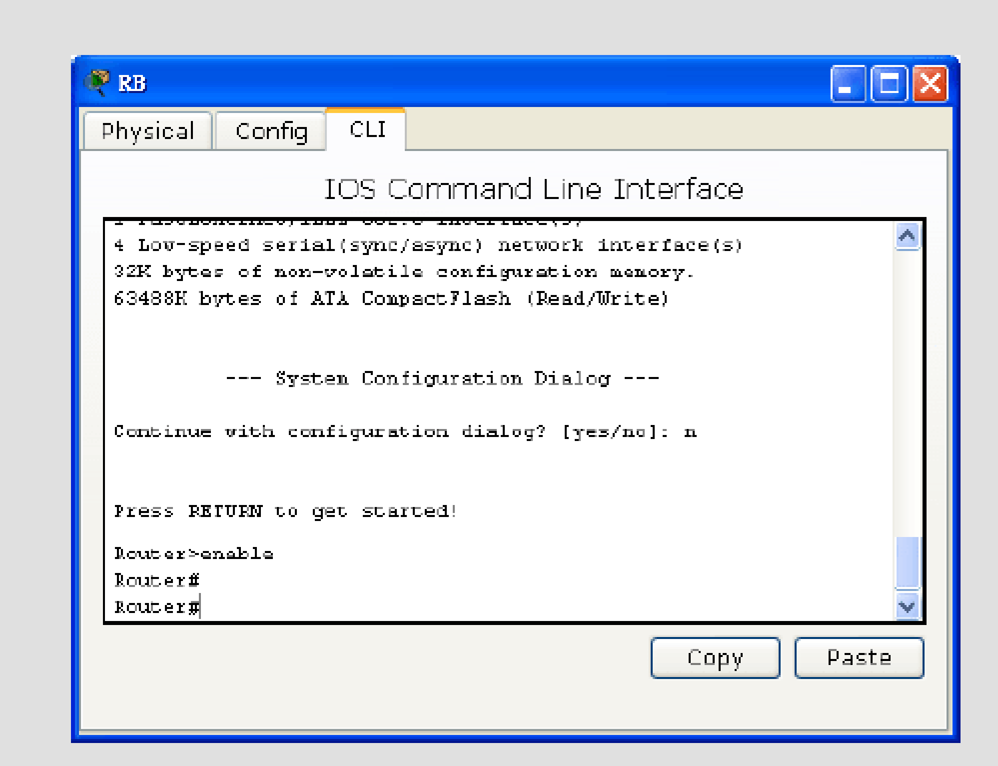


图 8-31　进入特权模式

（12）在特权模式下输入 configure terminal 命令，并按回车键，如图 8-32 所示。

（13）在全局配置模式下输入 interface s1/0 命令，并按回车键，如图 8-33 所示。

（14）在接口模式下输入 ip address 10.0.0.2 255.0.0.0 命令，并按回车键，如图 8-34 所示。

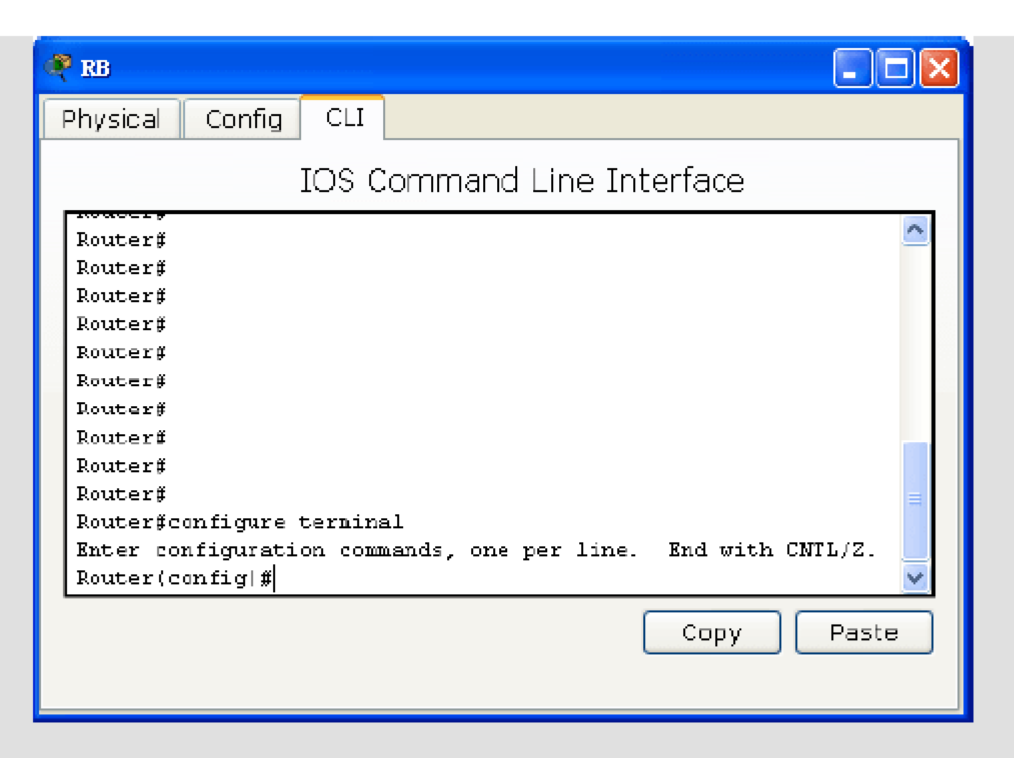


图 8-32　进入全局配置模式

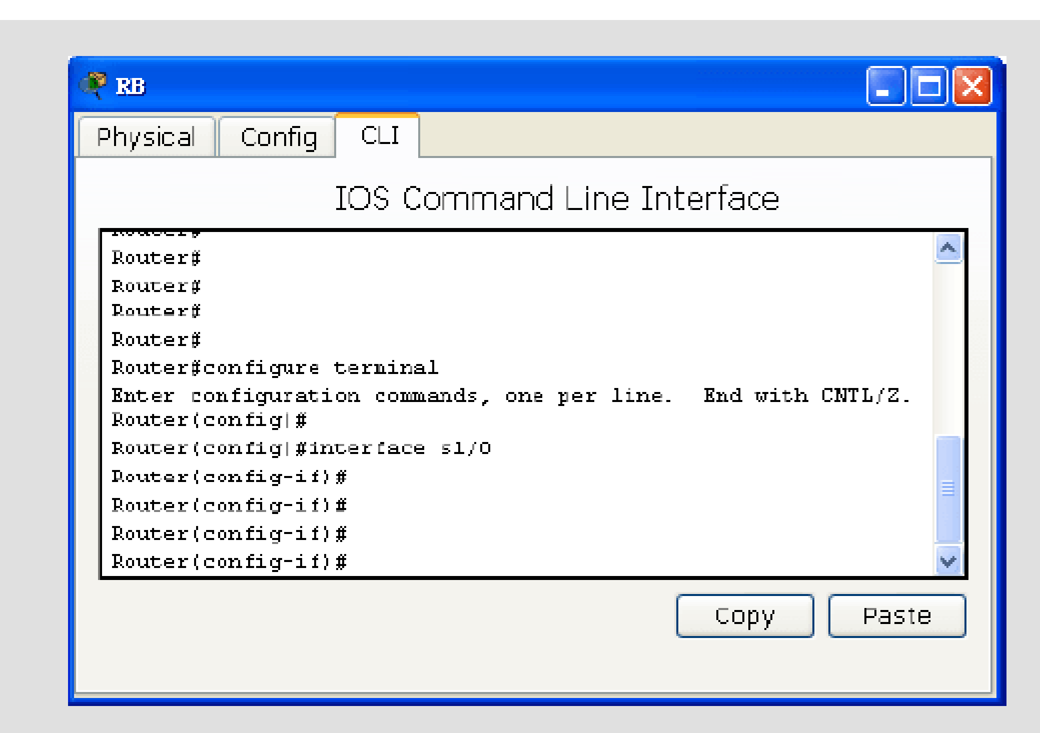


图 8-33　进入 s1/0 接口

（15）在该接口模式下输入 clock rate 128000 命令，并输入 no shutdown 命令，如图 8-35 所示。

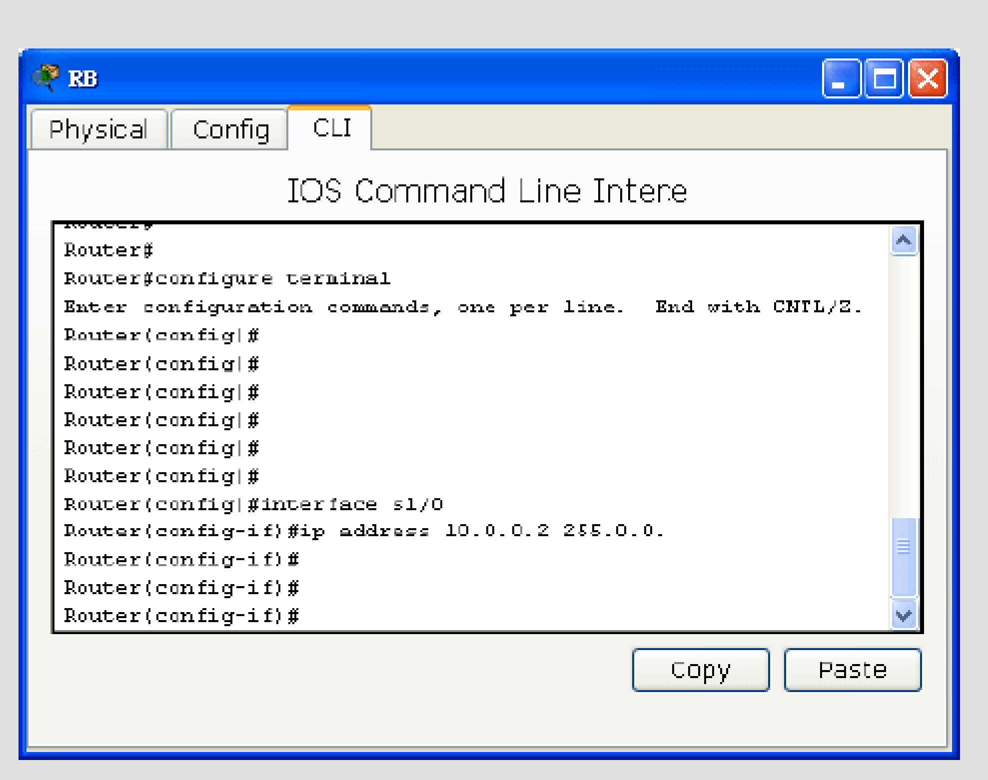


图 8-34　配置 s1/0 端口的 IP 地址

图 8-35　配置端口速率并开启端口

（16）在接口模式下输入 encapsulation ppp 命令，并按回车键，如图 8-36 所示。

（17）在该模式下输入 ppp pap sent-username cisco password 123456（发送验证信息）命令，并按回车键，如图 8-37 所示。

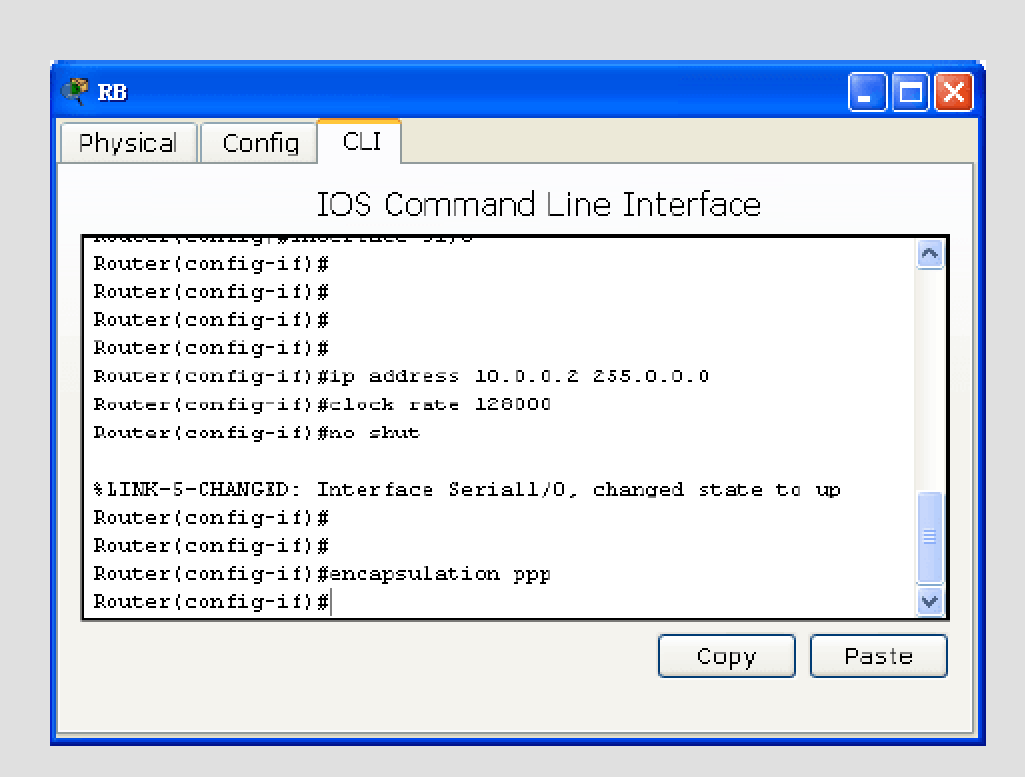


图 8-36　封装 ppp 协议

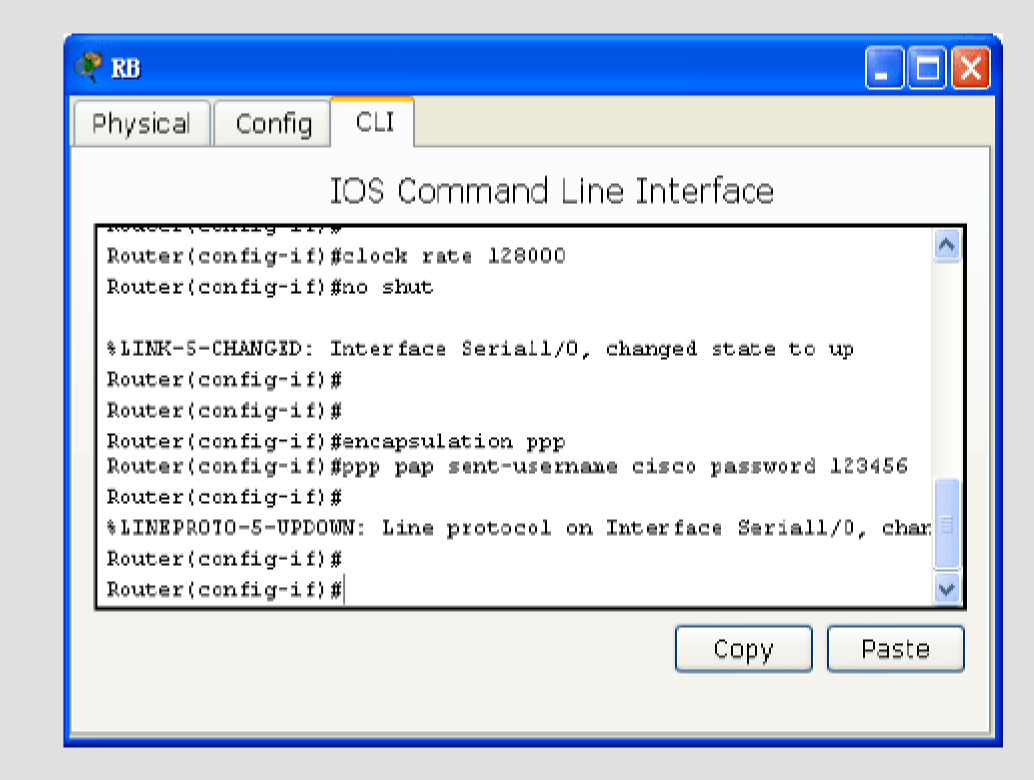


图 8-37　发送验证信息



RB 发送的用户名和密码必须与 RA 设置的用户名和密码相同。

第四篇　防火墙安全体系

第9章 防火墙基础

目前，防火墙技术已发展到一个非常成熟的阶段，成为用户网络和互联网相连的标准安全隔离设备。

由于 TCP/IP 协议是为网络互联而设计的开放性协议，在设计过程中可能缺乏安全措施的考虑。而防火墙就是用来保护用户网络，防止黑客利用 TCP/IP 协议内在安全弱点攻击网络设备和用户计算机。

在规划和使用防火墙来保护用户网络时，对防火墙的配置和使用环境进行设计，这就要求用户对防火墙有更多的了解。因此，本章对防火墙的基本技术、分类、功能和防火墙在不同环境下使用的建议进行详细的阐述。

本章学习要点：

- 防火墙功能及规则
- 防火墙分类
- 防火墙的体系结构
- 防火墙的主要应用

9.1 防火墙概述

防火墙（Firewall）是一款协助确保信息安全的设备，也可以理解为一个由软件和硬件设备组合而成的设备。它在内部网和外部网之间、专用网与公共网之间，构造成一个保护屏障，会依照特定的规则，允许或者限制传输的数据，从而保护内部网免受非法用户的入侵。

9.1.1 防火墙的基本概念

最初，防火墙是汽车中一个部件的名称。在汽车中，利用防火墙把乘客和引擎隔开，以便汽车引擎一旦着火，防火墙不但能保护乘客安全，同时还能让司机继续控制引擎。

但在网络应用中，所谓“防火墙”是一种将内部网和公众访问网（如 Internet）分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许“同意”的人和数据进入网络，同时将“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问网络。换句话说，如果不通过防火墙，公司内部的人就无法访问 Internet，Internet 上的人也无法和公司内部的人进行通信。

防火墙属于一种获取安全性方法的形象说法，也是一种计算机硬件和软件的结合，使

Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网络免受非法用户的入侵，防火墙主要由服务访问规则、验证工具、包过滤和应用网关组成。

整体来说，防火墙具有以下优点。

- 防火墙能强化安全策略。
- 防火墙能有效地记录 Internet 上的活动。
- 防火墙避免网络用户的暴露。防火墙能够用来隔开网络中一个网段与另一个网段，这样，能够防止影响一个网段的问题通过整个网络传播。
- 防火墙是一个安全策略的检查站。所有进出的信息都必须通过防火墙，防火墙便成为安全问题的检查点，使可疑的访问被拒之门外。

9.1.2 防火墙的功能

防火墙属于用户网络边界的安全保护设备。所谓网络边界也就是采用不同安全策略的两个网络连接处，比如家庭局域网和互联网之间连接或用户内网不同部门之间的连接等。防火墙的目的是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

通过防火墙可以对数据进行扫描，能够过滤掉一些攻击，以免所保护的网络中计算机受到破坏。另外，防火墙可以关闭不使用的端口而且能禁止特定端口的流出通信，封锁特洛伊木马；还可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。除此之外，防火墙还具有以下几点主要功能。

- **作为网络安全的屏障**

一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于防火墙可以对应用层协议进行监测和控制，所以网络环境变得更安全。如防火墙可以禁止不安全的 NFS（Network File System，网络文件系统）协议进出受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。同时，防火墙还可以保护网络免受基于路由的攻击，如 IP 路由（IP 数据包头中的源 IP 地址、目标 IP 地址信息）攻击。

- **强化网络安全策略**

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。

- **对网络存取和访问进行监控审计**

如果同一时间内某些访问都经过防火墙，那么该防火墙能够记录下这些访问并做出日志记录，同时也能提供网络使用情况的统计数据。当有可疑动作发生时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集网络中的使用和误用情况可以清楚防火墙是否能够抵挡攻击者的探测、攻击、控制等。并且网络使用统计对网络需求分析和威胁分析等来说也是非常重要的。

- **避免内部信息的外泄**

通过利用防火墙对内部网络的划分，可实现内部网络重点网段的隔离，从而限制局

部重点网络的安全对全局网络造成影响。并且，隐私是内部网络非常关心的问题，如内部网络中一些细小的信息，可能包含了有关安全的线索，而这些信息可能引起攻击者的兴趣，并暴露内部网络中的安全漏洞。

使用防火墙就可以隐蔽这些细小的信息，如 Finger、DNS等服务。其中，Finger 服务协议（返回一个指定主机上一个或多个用户的信息）中显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell（提供使用者使用界面的软件——命令解析器）类型等。

❑ **身份认证**

防火墙能够识别从外部网访问用户的身份，从而决定是否允许该用户访问内部网络，达到在用户端进行访问控制、对安全策略进行细化的目的。但是，身份认证（authentication）也会使网络通信的安全性降低，如防火墙必须在某些端口进行监听，这样很容易暴露防火墙的存在，会导致外部互联网的用户有机会在防火墙上面打开一个缺口虚拟专网。

9.1.3　防火墙的规则

防火墙是一种行之有效的网络安全机制，它是在网络内部和外部之间实施安全防范的系统。通过防火墙能够定义一个接入访问控制规则，要求并且保证仅当流量或数据匹配这个要求时才能穿越防火墙或者接入被保护的系统，从而实现管理和控制网络流量、保护资源的目的。

目前，防火墙中定义的规则主要分为进行包过滤型和代理服务型两种。

1. 包过滤型防火墙的规则

如图 9-1 所示，包过滤型防火墙一般有一个检查模块，该模块在操作系统或路由器转发数据包之前将拦截所有数据包，并对其进行验证，查看是否符合过滤规则。它的具体工作过程如下所述。

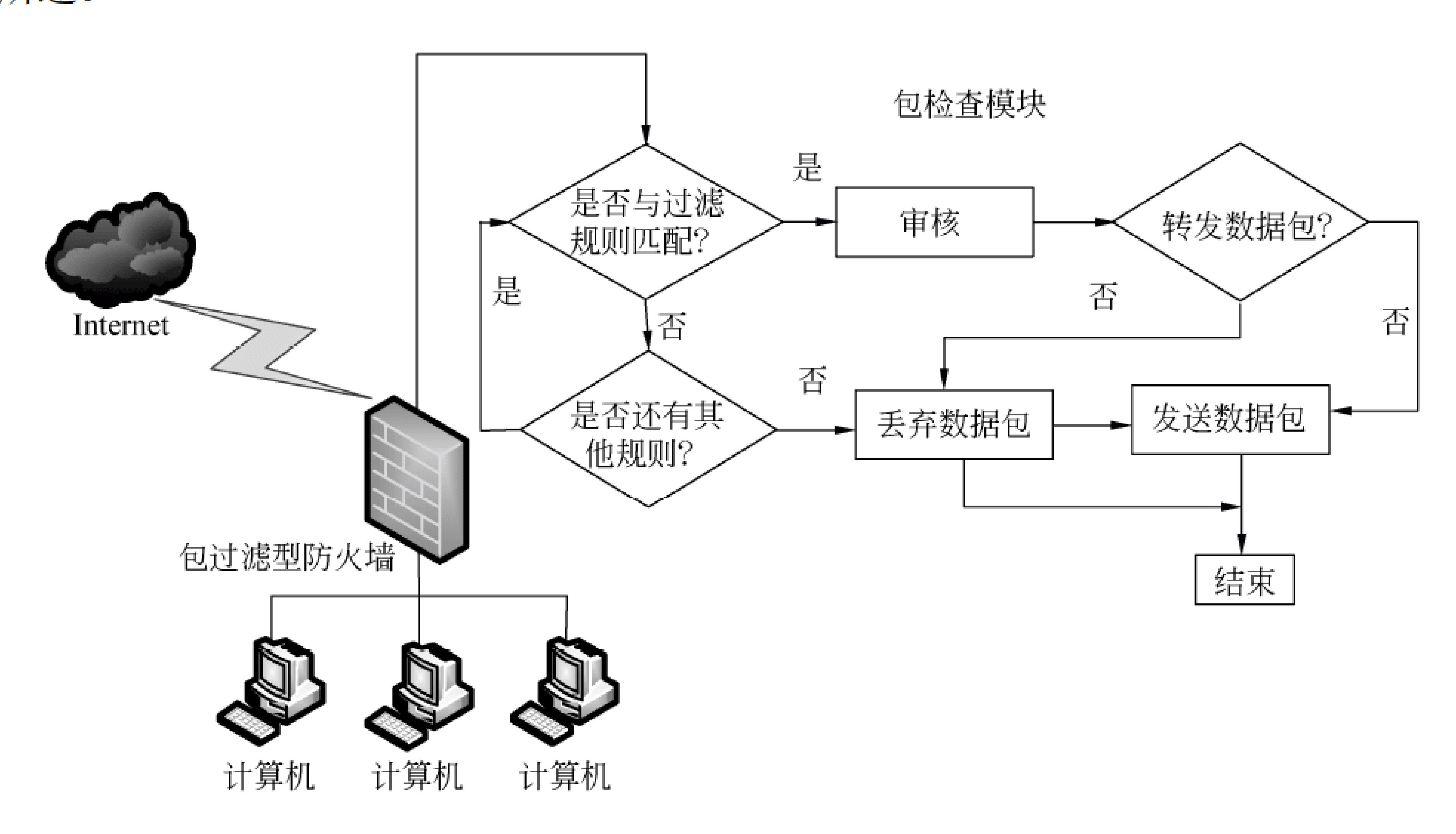


图 9-1　包过滤型防火墙工作规则图

- 数据包从外网传送到防火墙后，防火墙会在数据包从网络层传送到传输层之前，将数据包转发给包检查模块进行处理。
- 首先与第一个过滤规则比较。
- 如果第一个过滤规则相同，则对其进行审核，判断是否转发该数据包，这时如果审核结果是转发数据包，将数据包发送到传输层进行处理，否则将其丢弃。
- 如果与第一个过滤规则不同，则继续与第二个规则比较，如果相同则对它进行审核，过程与上步相同。
- 如果与第二个过滤规则不同，则继续与下一个过滤规则比较，直到与所有过滤规则比较完成。若不匹配所有过滤规则，则将数据包丢弃。

包检查器并不检查数据包的所有内容，它通常只检查下列几项。

- IP 源地址。
- IP 目标地址。
- TCP 协议或 UDP 协议的源端口号。
- TCP 协议或 UDP 协议的目标端口号。
- 协议类型。
- ICMP 消息类型。
- TCP 协议报头中的 ACK（确认）位。
- TCP 协议的序列号、确认号。

2. 代理服务型防火墙的规则

代理服务型防火墙主要是在应用层上实现防火墙功能，除了能够提供与传输有关的状态（IP 源地址、IP 目标地址）检测外，还能对应用状态（如服务类型）信息进行核对，从而更安全地保护网络。

也就是说，可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。图 9-2 为使用代理服务型防火墙的工作原理图。

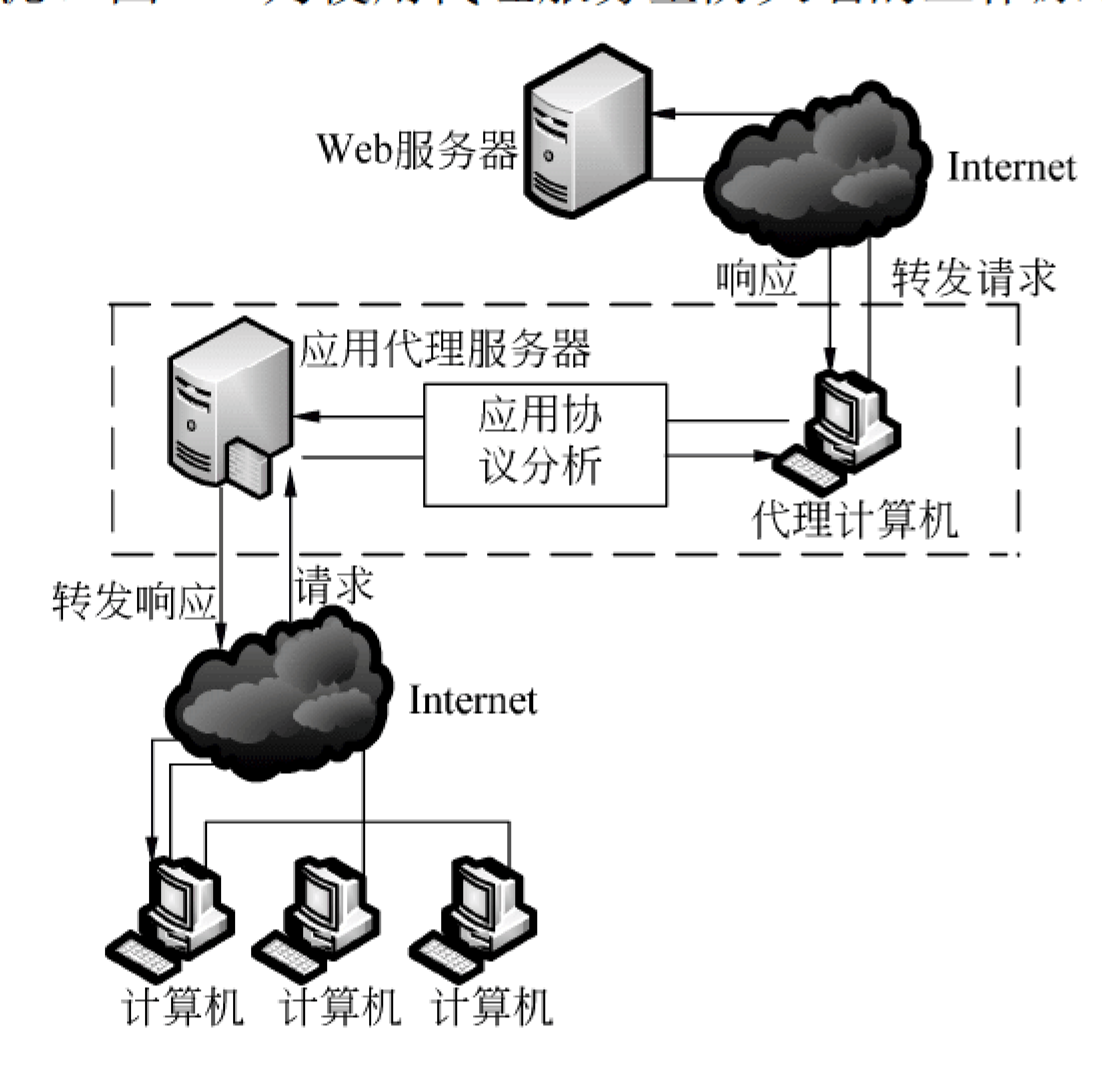


图 9-2　代理服务型防火墙的工作原理图

9.2 防火墙的分类

防火墙是一个位于计算机和它所连接的网络间的设备，目前，市场上的防火墙主要可以从软硬件、技术等方面来进行分类和选择。

9.2.1 按软硬件分类

从软硬件组成上来讲，可将防火墙分为硬件防火墙和软件防火墙两种。其中，硬件防火墙基于硬件平台设计，几乎与路由器同时产生，而软件防火墙为基于纯软件研发的防火墙，是防火墙应用技术普及的产物。

1. 硬件防火墙

最初的防火墙与平时所见到的集线器、交换机一样，都属于硬件产品，图 9-3 所示的是 3Com 公司的一款 3Com SuperStack 3 防火墙。它在外观上与网络中使用的集线器和交换机类似，只是只有少数几个接口，分别用于连接内、外部网络，这一特点由防火墙的基本作用决定。



图 9-3 3Com 防火墙系统产品图

另外，从防火墙的硬件性能上来分，还可将其分为低端硬件防火墙、高端硬件防火墙和高端服务器防火墙三类。

❑ **低端硬件防火墙**

硬件防火墙市场中的低端产品是一些需要进行一定配置的即插即用设备，就像普通的桌面交换机一样。这类低档设备经常集成了交换机和 VPN 功能。低端硬件防火墙适合小型公司和较大企业中内部使用。它们一般提供静态筛选功能和基本的远程管理功能。

低端硬件防火墙的优点在于成本低及配置简单（几乎不需要进行配置，即插即用）。也正是这类防火墙的优点决定了它的缺点，低端硬件防火墙只提供基本的防火墙功能，无法以并行的方式进行冗余，所以处理高吞吐量连接有限，可能会出现瓶颈。

❑ **高端硬件防火墙**

在高端硬件防火墙市场中，有适合企业或服务提供商的高性能、高适应性产品。这些产

品提供最好的保护，而不会降低网络的性能，还可以通过添加第二个作为运行的备份防火墙，以获得可用性的提高。

高端硬件防火墙可提供较高级别的入侵防护，同时对性能造成的影响最低。并且，将高端硬件防火墙连接在一起，以实现最佳的可用性和负载平衡。

另外，防火墙的硬件和软件均可以升级，以满足更高的防护要求。其中，硬件升级可能包括附加的以太网端口，而软件升级可能包括新入侵方法的检测。最后，高端硬件防火墙比低端硬件防火墙提供了更佳的远程管理功能等。

❑ **高端服务器防火墙**

高端服务器防火墙将防火墙功能添加到高端服务器中，在标准软件和软件系统上提供可靠快速的保护。此方法的好处是使用熟悉的硬件或软件，可以减少库存项目，简化培训和管理，提供可靠性和扩展性。

许多高端硬件防火墙产品是在运行行业标准操作系统和行业标准硬件平台上实现的，因此在技术上和性能上与服务器防火墙有一点差异。但是，因为操作系统仍然是可见的，所以服务器防火墙功能可以进行升级并且通过特殊技术使其具有更高的可用性和更高的性能。

服务器防火墙适用在特殊的硬件或软件平台上，因为防火墙使用相同的平台可以使管理任务更简单，并且缓存功能还非常有效。它的优点包括高性能（在一个性能合适的服务器上运行时，这些服务器可以提供较高级别的性能）和可用性、适应性和可扩展性好（由于这种防火墙运行在标准个人计算机硬件上）。

但是，服务器防火墙对硬件要求较高，即高端中央处理单元（CPU）、内存和网络接口。并且，服务器防火墙在服务器操作系统上运行，可能对该操作系统的其他软件带来安全隐患。

2．软件防火墙

随着防火墙应用的逐步普及和计算机软件技术的发展，为了满足不同层次用户对防火墙技术的需求，许多网络安全软件厂商开发出基于纯软件的防火墙，俗称“个人防火墙”。

个人防火墙是最常见的，通常为个人用户所选择，可以为个人计算机提供简单的防火墙功能。

虽然个人防火墙只为保护个人计算机而设计，但如果内部网络的其他计算机是通过安装个人防火墙的计算机与 Internet 相连接，那么它也可以起到保护内部网络的作用。不过，个人防火墙的性能有限，并会造成安装它的个人计算机的性能下降。这种保护机制通常不如专用防火墙解决方案有效，因为它们通常只限于阻止 IP、端口地址和一些比较简单的网络攻击，安全策略配置不是很灵活。

个人防火墙的优点主要在于价格很低甚至是免费的（微软已将个人防火墙系统集成到 Windows XP / Server 2003 版本中）且配置简单（个人防火墙产品通常可以使用直接的配置选项获得基本可使用的配置），各品牌的杀毒软件中也提供防火墙这一功能模块，如金山网镖、瑞星个人防火墙和傲盾 DDOS 防火墙（图 9-4）等。正是由于这些特点所以比较适合个人使用，特别适合使用便携计算机的移动用户。

个人防火墙的缺点也比较明显，主要有集中管理比较困难（需要在每个客户端进行配置，增加了管理开销）、仅具有基本控制（配置趋向于仅为静态数据包筛选和基于权限的应用程序阻止的组合）及性能限制（个人防火墙是为了保护个人计算机而设计的。在充当小型网络

的路由器的个人计算机上使用将导致性能下降）。并且由于其有限的性能和功能，在企业中，甚至小型附属办事处中不应考虑使用。

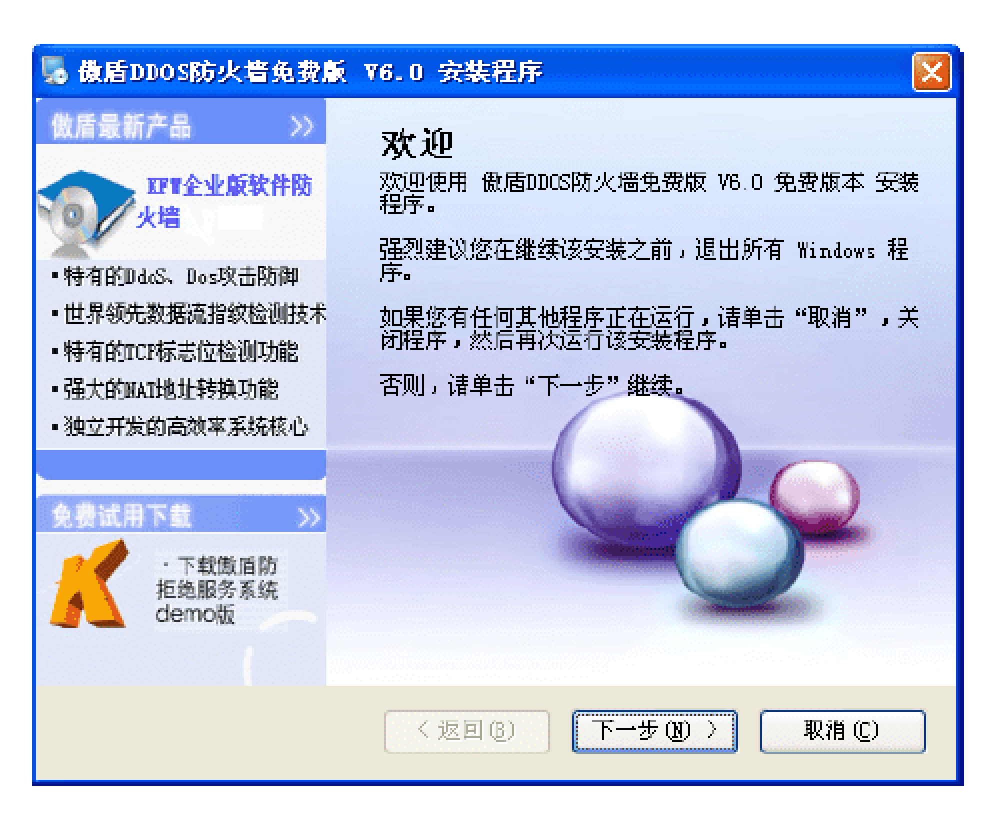


图 9-4 傲盾 DDOS 防火墙

9.2.2 按技术分类

目前，虽然出现了许多防火墙技术（包过滤、代理服务及网络地址转换等），但总体来讲可分为“包过滤型”和“应用代理型”两大类。

1. 包过滤型

包过滤（Packet Filtering）型防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址，目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤规则的数据包才被转发到相应的目的地，其余数据包则从数据流中丢弃。

包过滤方式是一种通用、廉价和有效的安全手段，因为它并不针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务，而且大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的，另外，它能够很大程度上满足绝大多数企业安全要求。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同版本，称为“第一代静态包过滤”和“第二代动态包过滤”。

❑ **第一代静态包过滤类型防火墙**

第一代静态包过滤类型防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制定。报头信息中包括 IP 源地址、IP 目标地址、传输协议（TCP、UDP、ICMP 等）、TCP/UDP 目标端口、ICMP 消息类型等。

❑ **第二代动态包过滤类型防火墙**

这类防火墙采用动态设置包过滤规则的方法，避免静态包过滤所具有的问题，进而发展成为包状态监测（Stateful Inspection）技术。采用这种技术的防火墙，对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。

包过滤方式的优点是不用改动客户机和计算机上的应用程序，因为它工作在网络层和传

输层，与应用层无关。但其弱点也很明显，过滤判断的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限的，且随着规则数目的增加，性能会受到很大的影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC 一类的协议。

另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常与应用网关配合使用，共同组成防火墙系统。

2. 应用代理型

应用代理（Application Proxy）型防火墙工作在 OSI 的最高层，即应用层。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

在代理型防火墙技术的发展过程中，它也经历了两个不同的版本，即第一代应用网关型代理防火和第二代自适应代理型防火墙。

- **第一代应用网关型防火墙**

第一代应用网关（Application Gateway）型防火墙，通过一种代理（Proxy）技术参与到一个 TCP 连接的全过程。从内部发出的数据包经过该防火墙处理后，就像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙，它的核心技术就是代理服务器技术。

- **第二代自适应代理（Adaptive Proxy）型防火墙**

这是最近才得到广泛应用的一种新防火墙类型，可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。

组成这种类型防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器（Dynamic Packet Filter），并在自适应代理服务器与动态包过滤器之间构成一个控制通道。当对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应 Proxy 的管理界面进行设置。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

代理服务类型防火墙的最突出的优点就是安全，因为它工作在最高层，可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。

另外，代理型防火墙采取的是一种代理机制，可以为每一种应用服务建立一个专门的代理（中间人）。因此，内外部网络之间的通信不是直接的，而都需先经过代理服务器审核，通过后再由代理服务器代为连接，根本不存在内、外部网络计算机直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。而包过滤类型的防火墙是很难彻底避免这一漏洞的。

对于代理防火墙来讲，它最大缺点则是速度相对比较慢，当用户对内外部网络网关的吞吐量要求比较高时，代理防火墙将会成为内外部网络之间的瓶颈。因为防火墙需要为不同的

网络服务建立专门的代理服务，用自己的代理程序为内、外部网络用户建立连接时需要时间，所以给系统性能带来了一些负面影响，但通常不会很明显。

9.2.3　防火墙的选择

防火墙作为防止黑客入侵的主要手段，已成为政府机关、企事业单位网络安全建设的必选设备。在有线数字电视的发展、数据网络建设和增值业务的应用等方面，同样离不开防火墙的保护。面对种类繁多的防火墙产品，用户应该如何选择呢?针对这一问题，用户可以将选择防火墙时涉及的基本原则和基本标准，以及应该考虑的企业特殊要求等作为参照。

1. 选择防火墙的基本原则

首先，应该明确目的，想要如何操作防火墙系统，即只允许想要的数据通过，比如某企业只需要电子函件服务，那么该企业将防火墙设置为只允许电子函件服务通过，而禁止 FTP、WWW 等服务，同时还允许多种业务通过防火墙，但要设置相应的监测、计量、注册和审核等。

其次，要考虑达到什么级别的监测和控制。根据网络用户的实际需要，建立相应的风险级别，随之便可形成一个需要监测、允许、禁止的清单，以此设置防火墙的各项功能。

然后，是费用问题。市场上，防火墙的售价极为悬殊，从几万元到数十万元，甚至上百万元。因为各企业用户使用的安全程度不尽相同，因此厂商所推出的产品也有所区分，甚至有些公司还推出类似模块化的功能产品，以符合各种不同企业的安全要求。安全性越高，实现越复杂，费用也越高，反之费用较低。这就需要对网络中需保护的信息和数据进行详细的经济性评估。

一般网络安全防护系统的造价，占需保护资源价值的 1%左右。所以在装配防火墙时，费用与安全性的折衷是不可避免的，这也就决定了“绝对安全”的防火墙是不存在的。但可以在现有经济条件下尽可能科学地配置各种防御措施，使防火墙充分发挥作用。

2. 选择防火墙基本标准

只要是能够限制数据包通行的网络设备，或安装在各种操作系统上的软件都可以用来当作防火墙。且可由不同特性的防火墙设计方式，来评估各种防火墙是否足够安全，以及能否满足企业的安全需求。具体说来，有以下几类指标。

❑ **防火墙的管理难易度**

防火墙的管理难易度，是防火墙能否达到目的的主要考虑因素之一。若防火墙的管理过于困难，则可能会造成设置的错误，反而不能达到其功能。

一般企业很少以已有的网络设备直接当作防火墙，是因为除了之前提到的包过滤（不能达到完全的控制）之外，还有设置工作困难、必须具备完整的知识才能排错等管理问题。

❑ **防火墙自身的安全性**

多数人在选择防火墙时，都将注意力放在防火墙如何控制连接以及防火墙支持多少种服务，但忽略防火墙同样是网络上的计算机之一，也可能存在安全问题。如果防火墙不能确保自身安全，即使防火墙的控制功能再强，还是不能完全保护内部网络。

大部分防火墙都安装在一般的操作系统上，如 UNIX、Windows 系统等。在防火墙计算机上执行的除了防火墙软件外，其他所有的程序、系统核心大多来自于操作系统本身的原有程序。所以，当防火墙上所执行的软件出现安全漏洞时，防火墙本身也将受到威胁。此时，任何防火墙控制机制都可能失效，因为当一个黑客取得了防火墙上的控制权后，黑客几乎可随意地修改防火墙上的存取规则（Access Rule），进而入侵更多的系统。因而，防火墙自身仍应有相当高的安全保护。

- **能否弥补其他操作系统的不足**

一款好的防火墙必须是建立在操作系统之前，而不是在操作系统之上，这样该操作系统有的漏洞可能不会影响到防火墙系统所提供的安全性。由于硬件平台的普及以及执行效率的因素，大部分企业均会把对外提供各种服务的服务器分散至许多操作平台上，但在无法保证所有主机安全的情况下，选择防火墙作为整体安全的保护者，这说明了操作系统提供的安全级别，并不一定会直接对整体安全造成影响，因为一款好的防火墙必须能弥补操作系统的不足。

- **能否为使用者提供不同平台的选择**

由于防火墙并非完全由硬件构成，而从软件（操作系统）所提供的功能及执行效率来看一定会影响到整体的效果；另外，使用者的操作意愿及熟悉程度也是必须考虑的重点之一。

因此，一款好的防火墙，不但本身要有良好的执行效率，还应该提供多平台的执行方式供使用者选择，毕竟使用者才是完全的控制者，应该选择一套符合现有环境需求的软件，而并不是因为软件的限制来改变现有环境。

- **能否向使用者提供完善的售后服务**

由于有新的产品出现，就有人会研究新的破解方法，所以一款好的防火墙提供者必须有一个庞大的组织作为使用者的安全后盾，也应该有众多的使用者所建立的口碑为防火墙作见证。

3. 企业的特殊需求

企业安全政策中往往有些特殊需求，并不是每一款防火墙都会提供的，这也常常成为选择防火墙的考虑因素之一。常见的需求如下所述。

- **IP 地址转换**

进行 IP 地址转换（IP Address Translation）有两个好处，其一是隐藏内部网络真正的 IP 地址，这可以使黑客（Hacker）无法直接攻击内部网络；另一好处是可以让内部使用保留的 IP 地址，这对许多 IP 地址不足的企业是有益的。

- **双重 DNS**

当内部网络使用没有注册的 IP 地址，或是防火墙进行 IP 地址转换时，DNS 也必须进行转换。因为，同样一台计算机在内部的 IP 地址与转换后的 IP 地址将会不同，有的防火墙会提供双重 DNS，有的则必须在不同计算机上各安装一个 DNS。

- **虚拟企业网络**

VPN 可在防火墙与防火墙或移动客户间，对所有网络传输的内容加密，建立一个虚拟通道，让通信双方感觉是在同一个网络上，可以安全且不受拘束地互相存取。这对于总公司与分公司之间或公司与外出的员工之间，需要直接联系，又不愿花费大量金钱特意申请专线或

用长途电话拨号连接时，将会非常实用。

❑ 扫毒功能

大部分防火墙，可以与防病毒防火墙搭配实现扫毒功能，还有一些防火墙则可以直接集成扫毒功能，差别只是扫毒工作是由防火墙完成，或是由另一台专用的计算机完成。

防火墙是企业网络安全问题的流行方案，即把公共数据和服务置于防火墙外，使其对防火墙内部资源的访问受到限制。而一款好的防火墙，不但应该具备包括检查、认证、警告、记录的功能，并且能够为使用者解决可能遇到的困境，如 IP 地址不足形成的 IP 地址转换的问题，信息加密/解密的问题等，这也是选择防火墙时必须考虑的重点之一。

9.2.4　网管心得——防火墙与路由器的安全性比较

防火墙已经成为企业网络建设中的一个关键组成部分。但是仍有许多用户不理解，网络中已经有了路由器，并且可以实现一些简单的包过滤功能，但为什么还要用防火墙呢？实际上，无论从设备产生和存在的背景、核心技术、安全策略制定的复杂程度、对性能的影响、审计功能的强弱，还是在防范攻击能力方面都有一定的差别。

在此，针对 NetEye 防火墙，与最具代表性的 Cisco 路由器在安全方面进行对比。

1. 两者产生和存在的背景不同

路由器的产生基于对网络数据包路由，其作用是将不同网络的数据包进行有效的路由，但对于路由的原因、是否应该路由、路由后是否有问题等根本不关心，所关心的是能否将不同的网段的数据包进行路由从而进行通信。

防火墙产生于人们对于安全性的需求，数据包是否可以正确地到达、到达的时间、方向等并不是防火墙关心的重点，其重点是该数据包是否应该通过、通过后是否会对网络造成危害。

2. 核心技术不同

Cisco 路由器核心的 ACL 列表是基于简单的包过滤，但 NetEye 防火墙则是基于状态包过滤的应用层信息流过滤。

图 9-5 所示为一个最简单的应用，企业内网的一台服务器，通过路由器对外网提供服务（假设提供服务的端口为 TCP 1455）。为了保证安全性，在路由器上需配置规则，当外部用户访问内部服务时，只允许客户端（client）访问服务器（server）的 TCP 1455 端口，其他拒绝。

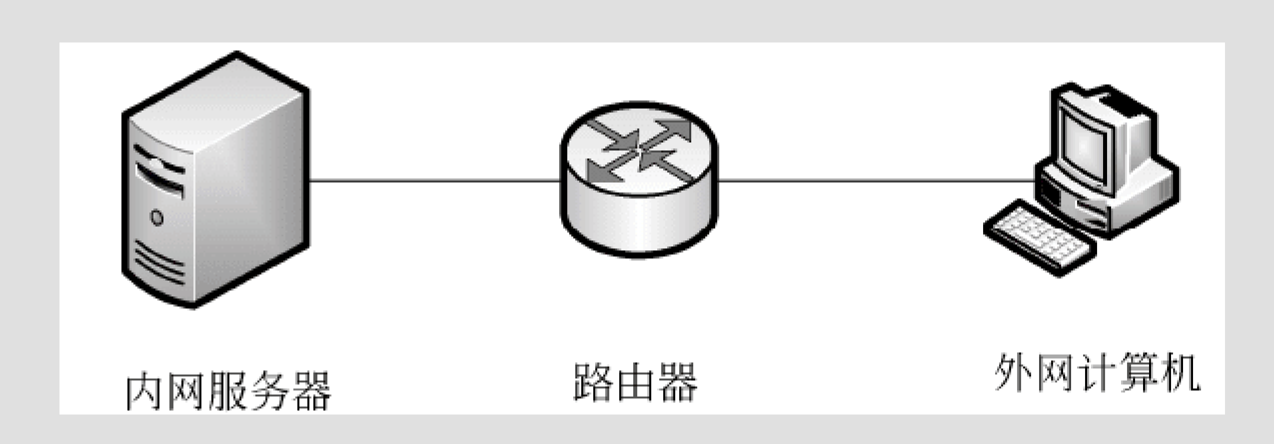


图 9-5　路由器安全设置

针对该配置，存在的安全隐患如下所述。

- IP 地址欺骗（使连接非正常复位）。
- TCP 欺骗（会话重放和劫持）。

存在上述隐患的原因是，路由器不能监测 TCP 的状态。如果在内网客户和路由器之间放上 NetEye 防火墙，由于 NetEye 防火墙能够检测 TCP 的状态，并且可以重新随机生成 TCP 的序列号，那么就可以彻底消除这样的隐患。同时，NetEye 防火墙的一次性口令认证客户端功能，能够在对应用完全透明的情况下，实现对用户的访问控制。

虽然，路由器的“Lock-and-Key”（动态访问控制列表）功能能够通过动态访问控制列表的方式，实现对用户的认证，但该特性需要路由器提供 Telnet 服务，用户在使用时也需要先 Telnet 到路由器上，使用起来很不方便，同时也不够安全（开放的端口为黑客创造了机会）。

3. 安全策略制定的复杂程度不同

路由器的默认配置对安全性的考虑不够，需要一些高级配置才能达到一些防范攻击的作用，且安全策略的制定绝大多数都是基于命令行的，其针对安全性规则的制定相对比较复杂，配置出错的概率较高。

NetEye 防火墙的默认配置可以防止各种攻击，达到即用即安全，安全策略的制定是基于全中文的 GUI（用户界面）的管理工具，其安全策略的制定人性化，配置简单、出错率低。

4. 对性能的影响不同

路由器被设计用来转发数据包，并不是专门设计作为全特性防火墙，所以用于进行包过滤时，需要进行的运算非常大，对路由器的 CPU 和内存的需要都非常大，而路由器由于其硬件成本比较高，其高性能配置时硬件的成本都比较大。

NetEye 防火墙的硬件配置非常高（采用通用的 Intel 芯片，性能高且成本低），其软件也为数据包的过滤进行了专门的优化，其主要模块运行在操作系统的内核模式下，设计时特别考虑安全问题，其进行数据包过滤的性能非常高。

由于路由器是简单的包过滤，包过滤的规则条数的增加，NAT 规则的条数的增加，对路由器性能的影响都相应地增加，而 NetEye 防火墙采用的是状态包过滤规则条数，NAT 的规则数对性能的影响接近于零。

5. 审计功能强弱的差异

路由器本身没有日志、事件的存储介质，只能通过采用外部的日志服务器（如 syslog，trap）等来完成对日志、事件的存储；没有审计分析工具，对日志、事件的描述，采用不太容易理解的语言。而且，路由器对攻击等安全事件的响应不完整，对于很多的攻击、扫描等操作不能产生准确及时的事件。另外，审计功能的弱化，使管理员不能对安全事件进行及时、准确的响应。

NetEye 防火墙的日志存储介质有两种，包括本身的硬盘存储和单独的日志服务器。针对这两种存储，均提供了强大的审计分析工具，使管理员可以非常容易分析出各种安全隐患；其次，NetEye 防火墙还具有实时监控功能，可在线监控通过防火墙的连接，同时能够捕捉数据包进行分析，为排除网络故障提供了方便。

6. 防范攻击能力不同

对于 Cisco 的路由器，其普通版本不具有应用层的防范和入侵实时检测等功能，若要使其具有这些功能，则需升级 IOS 为防火墙特性集，此时不但要承担软件的升级费用；同时由于这些功能都需要进行大量的运算，还需要进行硬件配置的升级，进一步增加了成本，而且很多厂家的路由器不具有这样的高级安全功能。

综上所述，用户的网络拓扑结构简单与否、用户应用程序的难易程度不是决定是否应该使用防火墙的标准，决定用户是否使用防火墙的一个根本条件是用户对网络安全的需求。

即使用户的网络拓扑结构和应用都非常简单，使用防火墙仍然是必需的和必要的；如果用户的环境、应用比较复杂，那么防火墙将能够带来更多的好处，防火墙将是网络建设中不可或缺的一部分，对于通常的网络来说，路由器将是保护内部网的第一道关口，而防火墙将是第二道关口，也是最为严格的一道关口。

9.3 防火墙的体系结构

堡垒主机在防火墙体系结构中起着至关重要的作用，它专门用来击退攻击行为。网络防御的第一步是寻找堡垒主机的最佳位置，堡垒主机为内网和外网之间的所有通道提供一个阻塞点。没有堡垒主机就不能连接外网，同样外网也不能访问内网。如果通过堡垒主机来集中网络权限，就可以更轻松地配置软件来保护网络。

针对各种类型的防火墙来讲，其应用结构主要可分为包过滤型结构、双宿网关结构、屏蔽主机结构和屏蔽子网结构。

1. 包过滤型结构

包过滤型结构是通过专用的包过滤路由器，或是安装了包过滤功能的普通路由器来实现的。包过滤型结构对进出内部网络的所有信息进行分析，按照一定的安全策略对这些信息进行分析与限制，如图 9-6 所示。

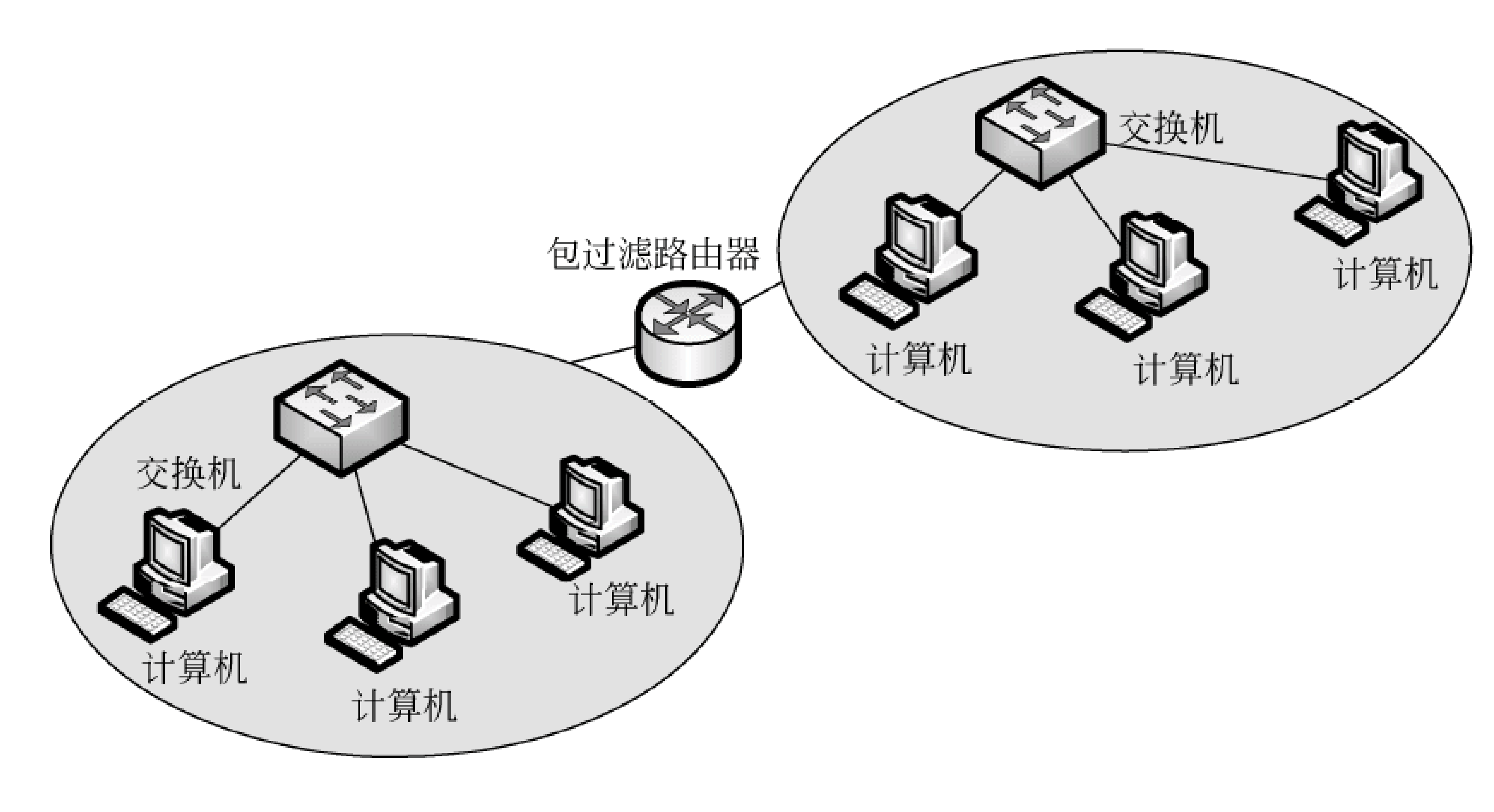


图 9-6　包过滤型结构

包过滤型结构处理速度快、费用低且对用户透明，结构简单，便于管理。但是，包过滤型结构对于包过滤的判断只限于数据包的头信息，并不涉及包的内容，所以它只能阻止部分IP 欺骗的数据包。另外，包过滤结构的日志功能有限，不能从日志中发现黑客的攻击记录，并且配置比较烦琐。

2．双宿 / 多宿主机模式

连接了两个网络的多宿主机（具有多个网络连接的主机）称为双宿主机（Dual-Homed / Multi-Homed Firewall）。多宿主机是具有多个网络接口卡的主机，每个接口都可以和一个网络连接。因为它能在不同的网络之间进行数据交换，因此也称为网关。双宿网关结构是用一台装有两块网卡的主机作为防火墙，将外部网络与内部网络实现物理上的隔开，这台处于防火墙关键部位且运行应用级网关软件的计算机系统称为堡垒主机。图 9-7 为双宿网关结构。

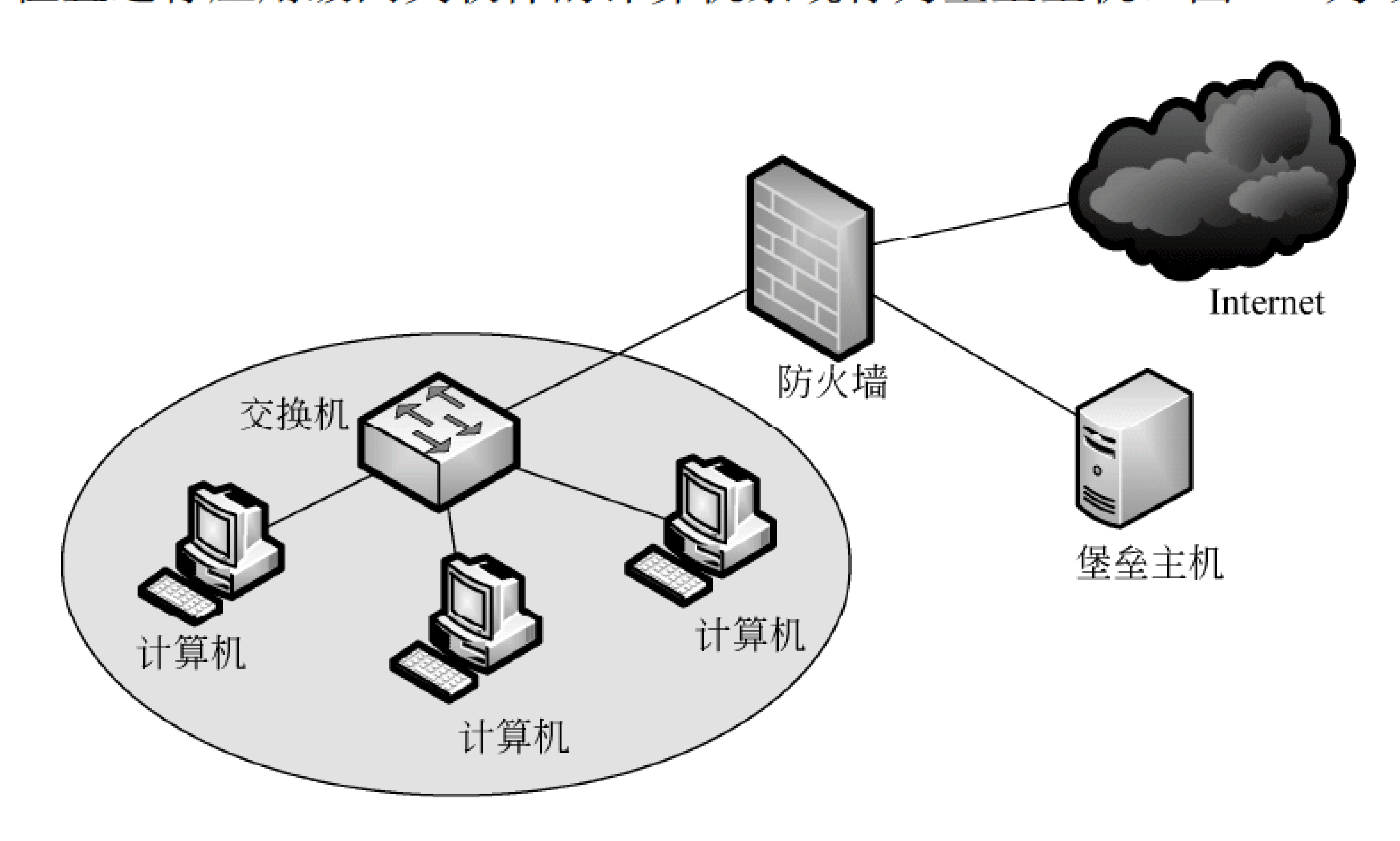


图 9-7　双宿 / 多宿主机模式

双宿网关的结构的安全性较高，但入侵者一旦得到了双宿网关的访问权，即可入侵内部网络。所以在设置该应用级网关时应该注意以下几点。

- 在该应用级网关的硬件系统上运行安全可信任的安全操作系统。
- 安全应用代理软件，保留 DNS、FTP、SMTP 等必要的服务，删除不必要的服务与应用软件。
- 设计应用级网关的防攻击方法与被破坏后的应急方案。

3．屏蔽主机结构

屏蔽主机防火墙（Screened Firewall）结构将所有的外部主机强制与一个堡垒主机相连，从而不允许它们直接与内部网络的主机相连，如图 9-8 所示。因此，屏蔽主机结构是由包过滤路由器和堡垒主机组成的。屏蔽主机实现了网络层和应用层的安全，并且安全性较高。但是堡垒主机一旦被绕过，则堡垒主机和其他内部网络的主机之间没有任何保护网络安全的措施，内网将暴露。

外部某主机想要访问内部网络，该主机发送了一个请求包。该请求包被包过滤路由器接收到以后，先从数据包中得到目的地址，检查这个 IP 地址是否合法。如果合法，再查询转发

路由表，得到该 IP 地址相应的转发目的地址即为堡垒主机 IP 地址，则将该数据包转发到这个堡垒主机。然后，再通过其判断这个请求的主机是否位于该内部网络的合法用户。如果合法，则将该请求数据包转发到内网。这个数据包实际的转发路径应为“客户主机—包过滤路由器—堡垒主机—被请求的内网计算机”。如果内部网络的主机要访问外部网络的服务器，也要经过堡垒主机与包过滤路由器的检查。

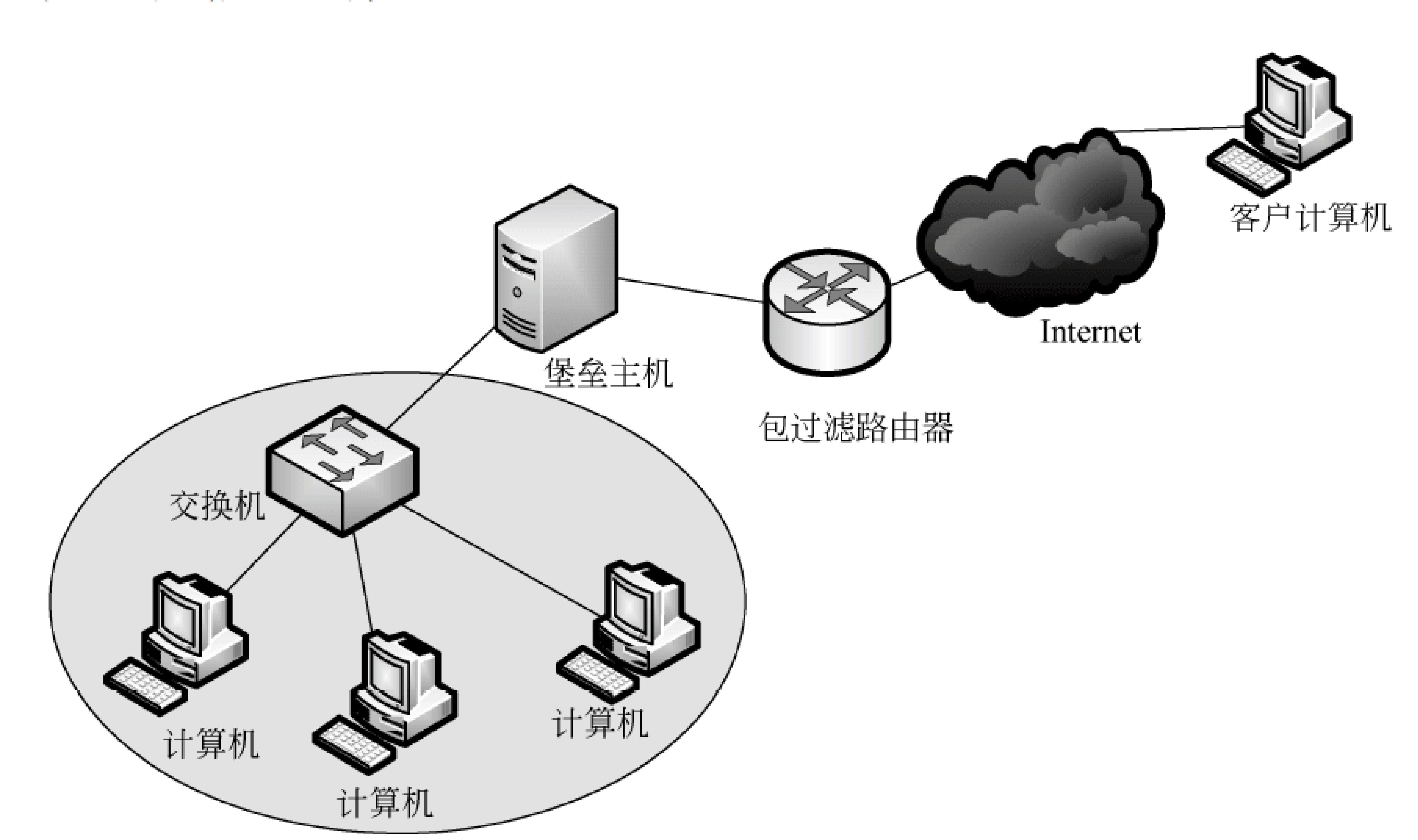


图 9-8　屏蔽主机结构

4. 屏蔽子网结构

子网屏蔽防火墙体系（Screened Subnet Mode Firewall）结构添加额外的安全层到主机屏蔽体系结构，即通过添加周边网络更进一步地把内部网络与外网隔离，支持网络层和应用层的安全功能。

通常，堡垒主机是网络上最容易受攻击的机器。任凭用户如何保护，它仍有可能被突破或入侵，因为没有主机是绝对安全的。

在主机屏蔽体系中，用户的内部网络对堡垒主机没有任何防御措施，如果黑客成功入侵到主机屏蔽体系结构中的堡垒主机，那就可以毫无阻挡地进入内部网络。通过在周边网络上隔离堡垒主机，能减少在堡垒主机上入侵的影响。可以说它只给入侵者一些访问的机会，但不是全部。

屏蔽子网体系结构的最简单的形式为使用两个屏蔽路由器，位于堡垒主机的两端，一端连接内网，一端连接外网，如图 9-9 所示。为了入侵这种类型的体系结构，入侵者必须穿透两个屏蔽路由器。即使入侵者控制了堡垒主机，仍然需要通过内网端的屏蔽路由器才能到达内网。

在构造防火墙体系时，一般很少使用单一的技术，通常都是多种解决方案的组合。这种组合主要取决于网管中心向用户提供什么服务，以及网管中心能接受什么等级的风险。还要看投资经费、投资大小、技术人员的水平和时间等问题。一般包括下面几种形式。

图 9-9　屏蔽子网结构

- 使用多个堡垒主机。
- 合并内部路由器和外部路由器。
- 合并堡垒主机和外部路由器。
- 合并堡垒主机和内部路由器。
- 使用多个内部路由器。
- 使用多个外部路由器。
- 使用多个周边网络。
- 使用双宿主主机与屏蔽子网。

9.4　防火墙的主要应用

网络中，防火墙的部署并不只是将它的 LAN 端口和 WAN 端口分别与局域网线路连接和外部网络线路连接这么简单，要根据实际的应用需求而定，并不是统一的，如工作在何种模式、配置规则是否需要修改等。

9.4.1　防火墙的工作模式

目前，防火墙能够工作在路由模式、透明模式、混合模式这 3 种模式下。若防火墙以网络层对外连接（接口具有 IP 地址），则认为防火墙工作在路由模式下；若防火墙通过数据链路层对外连接（接口无 IP 地址），则防火墙工作在透明模式下；若防火墙同时具有工作在路由模式和透明模式的接口（某些接口具有 IP 地址，某些接口无 IP 地址），则防火墙工作在混合模式下。下面分别进行介绍。

1. 路由模式

当防火墙位于内部网络和外部网络之间时，需要将防火墙与内部网络、外部网络以及

DMZ3 个区域相连的接口，分别配置成不同网段的 IP 地址，重新规划原有的网络拓扑，此时相当于一台路由器。如图 9-10 所示，防火墙的 Trust 区域接口与公司内部网络相连，Untrust 区域接口与外部网络相连。并且 Trust 区域接口和 Untrust 区域接口分别处于两个不同的子网中。

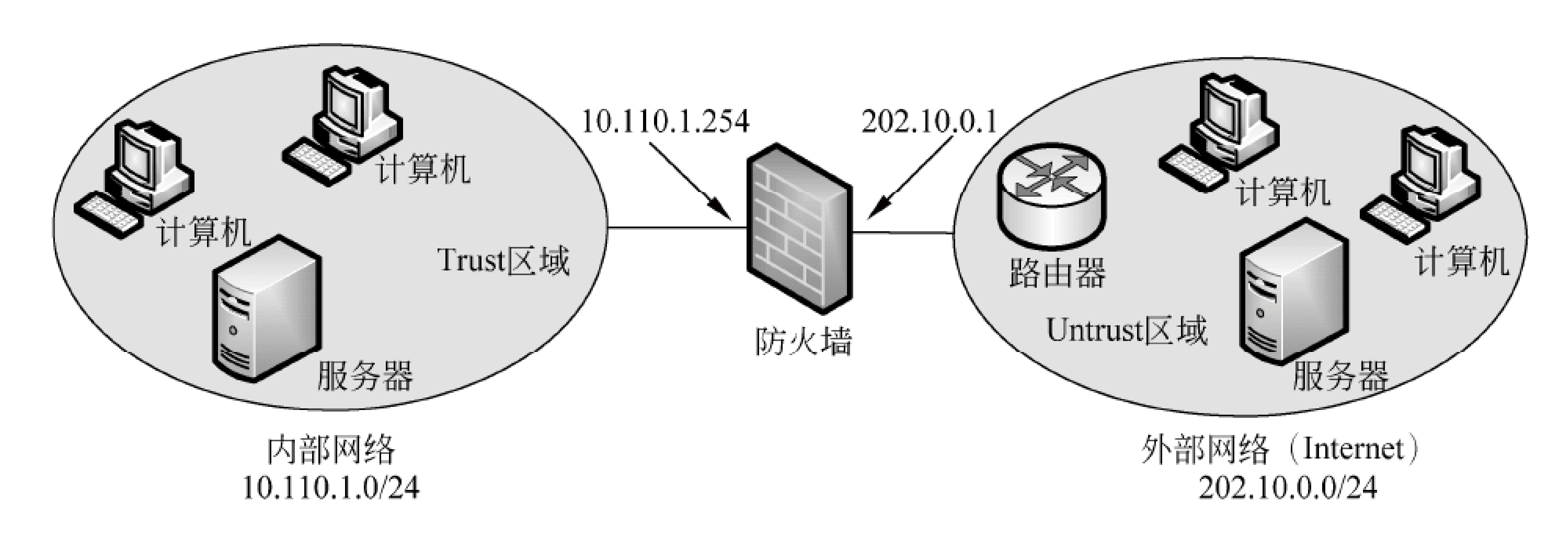


图 9-10　路由模式组网图

采用路由模式时，可以实现 ACL（访问列表）包过滤、aspf 动态过滤（application specific packet filter，针对应用层的包过滤）、NAT 转换等功能。然而，路由模式需要对网络拓扑进行修改（内部网络用户需要更改网关、路由器需要更改路由配置等），此操作较为复杂，因此在使用该模式时需权衡利弊。

2. 路由模式工作过程

防火墙工作在路由模式时，所有接口都配置 IP 地址，各接口所在的安全区域属于三层区域，即配置 IP 地址的接口所在的区域是三层区域。且不同三层区域相关的接口连接的外部用户属于不同的子网。

当报文在三层区域的接口间进行转发时，根据报文的 IP 地址来查找路由表。此时，防火墙则充当路由器。但防火墙与路由器存在不同，防火墙中 IP 报文还需送到上层（传输层）进行相关过滤等处理，通过检查会话表或 ACL 规则以确定是否允许该报文通过。

此外，还将进行其他防攻击检查，路由模式的防火墙支持 ACL 规则检查、aspf 状态过滤、防攻击检查、流量监控等功能。

3. 透明模式

如果防火墙采用透明模式进行工作，则可以避免因改变拓扑结构造成的麻烦，此时防火墙对于子网用户和路由器来说是完全透明的。也就是说，用户完全感觉不到防火墙的存在。

采用透明模式时，只需在网络中像放置网桥（bridge）一样插入一台防火墙设备即可，无需修改任何已有的配置。与路由模式相同，IP 报文同样经过相关的过滤检查（但是 IP 报文中的源或目的地址不会改变），内部网络用户依旧受到防火墙的保护。防火墙透明模式的典型组网方式如图 9-11 所示。

如图 9-11 所示，防火墙的 Trust 区域接口与公司内部网络相连，Untrust 区域接口与外部网络相连，需要注意的是内部网络和外部网络必须处于同一个子网。

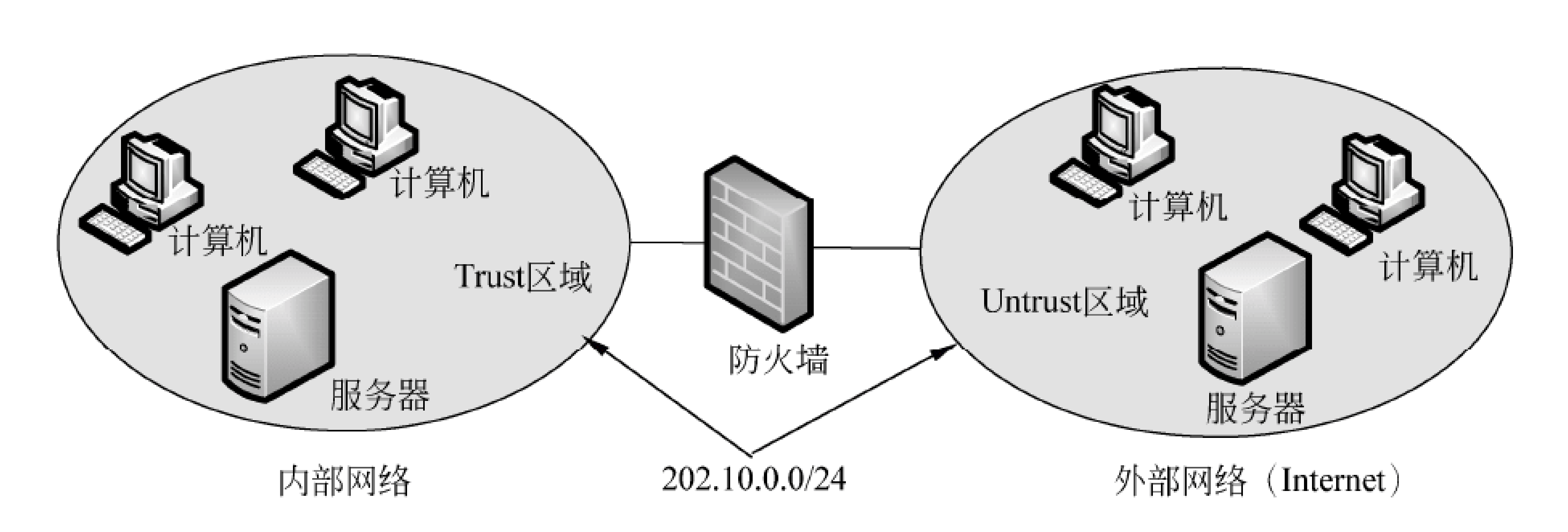


图 9-11 透明模式的组网方式

4. 透明模式工作过程

防火墙工作在透明模式（也可以称为桥模式）下，此时所有接口都不能配置 IP 地址，接口所在的安全区域为二层区域，且与二层区域相关接口连接的外部用户同属一个子网。

当报文在二层区域的接口间进行转发时，需要根据报文的 MAC 地址来寻找出接口，这时防火墙充当透明网桥。不过防火墙与网桥存在不同，防火墙中 IP 报文还需送到上层进行相关过滤等处理，通过检查会话表或 ACL 规则以确定是否允许该报文通过。另外，还要完成其他防攻击检查。透明模式的防火墙支持 ACL 规则检查、aspf 状态过滤、防攻击检查、流量监控等功能。

工作该模式下的防火墙在数据链路层连接局域网（LAN），网络终端用户无需为连接网络而对设备进行特别配置，类似一个局域网交换机来进行网络连接。透明模式工作过程分为如下几个阶段。

❑ 获取地址表过程

采用透明模式，防火墙依据 MAC 地址表（由 MAC 地址和接口两部分组成）进行转发。透明模式防火墙必须获取 MAC 地址和接口的对应关系。

透明模式防火墙要获取 MAC 地址和接口对应关系，首先为广播消息包过程。即在它与物理网段相连时，会监测该物理网段上的所有以太网帧，一旦监测到某个接口上节点发来的以太网帧，就提取出该帧的源 MAC 地址，并将该 MAC 地址与接收该帧的接口之间的对应关系加入到 MAC 地址表中，如图 9-12 所示。

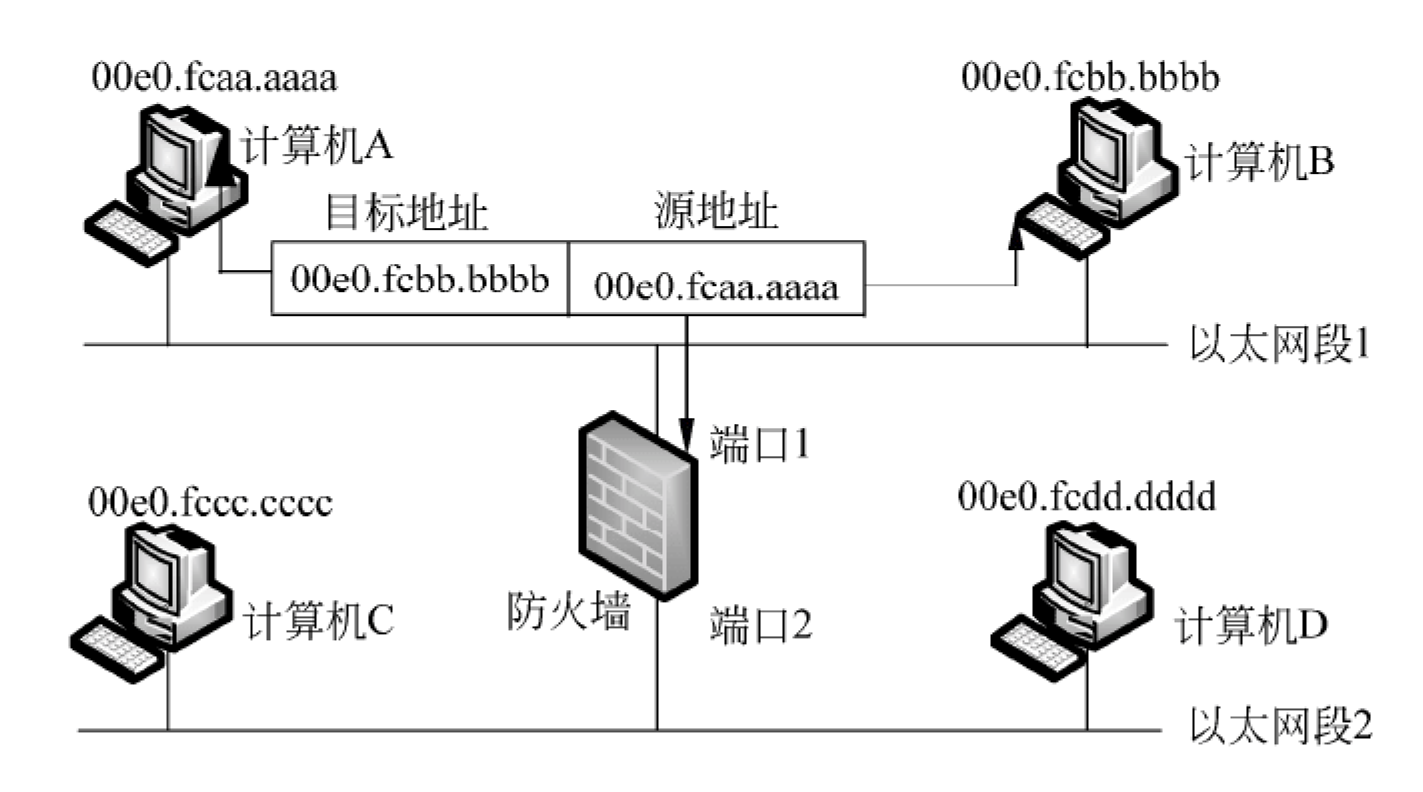


图 9-12 广播消息包

A、B、C 和 D 四台计算机分布在两个局域网中，以太网段 1 与透明模式防火墙端口 1 相连，以太网段 2 与端口 2 相连。某一时刻，当工作站 A 向工作站 B 发送以太网帧时，透明模式防火墙和计算机 B 都将收到这个帧。

其次，是透明模式防火墙反向学习计算机 A 的 MAC 地址和端口对应关系过程。当防火墙收到这个以太网帧后，就知道计算机与防火墙端口 1 相连（因为从端口 1 收到了该帧），此时计算机 A 的 MAC 地址与防火墙端口 1 的对应关系，就被加入到 MAC 地址表中，如图 9-13 所示。

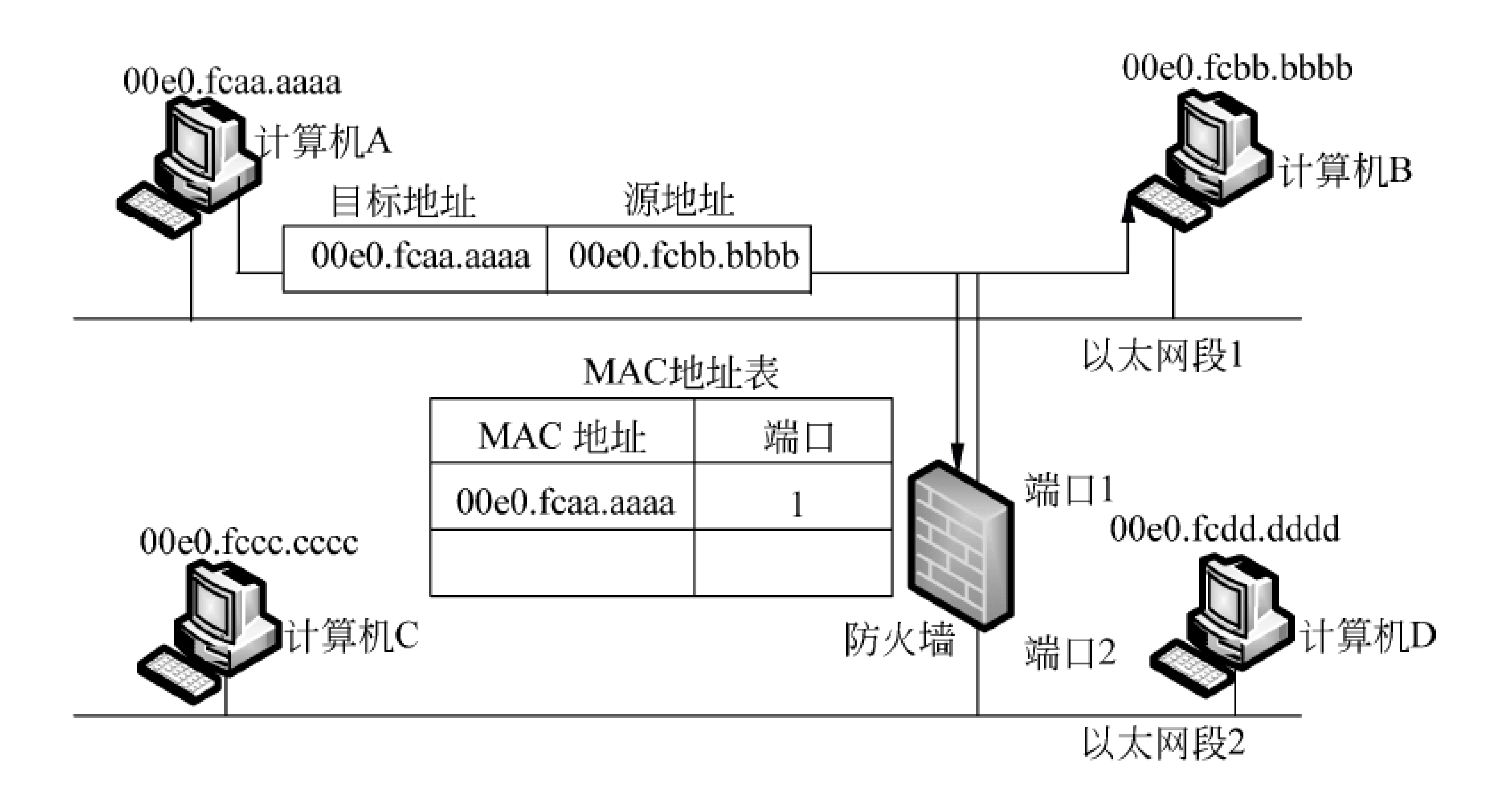


图 9-13　反向学习计算机 A 的 MAC 地址与端口对应关系

然后，则为透明模式防火墙反向学习计算机 B 的 MAC 地址和端口对应关系过程。当计算机 B 对计算机 A 的以太网帧作出响应后，防火墙也能监测到计算机 B 回应的以太网帧，并知道计算机 B 也与防火墙端口 1 相连（因为从接口 1 收到了该帧）。此时，计算机 B 的 MAC 地址与防火墙端口 1 的对应关系也被加入到 MAC 地址表中，如图 9-14 所示。

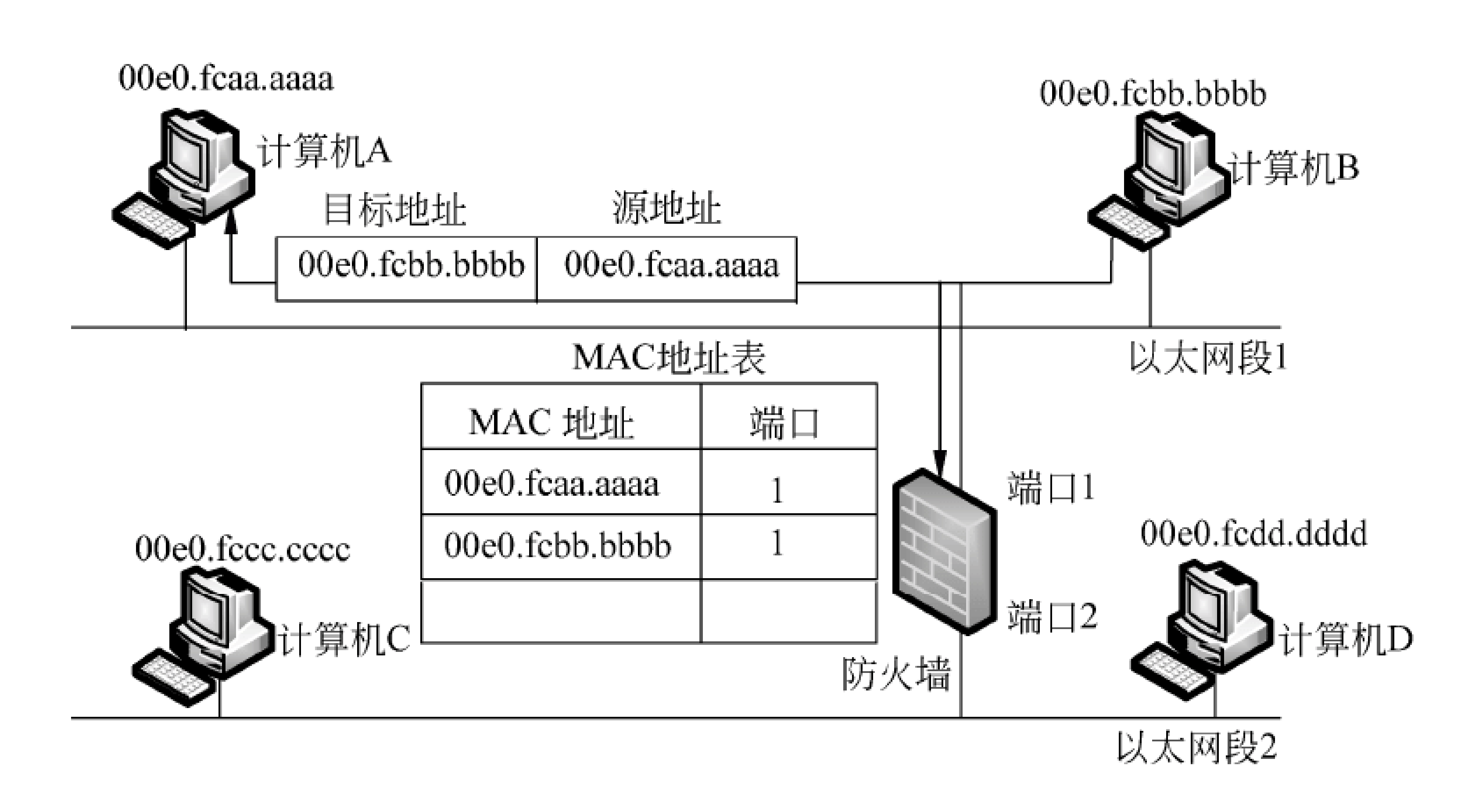


图 9-14　反向学习计算机 B 的 MAC 地址与端口对应关系

反向学习过程一直进行，直到所有 MAC 地址与接口的对应关系（本例中为计算机 A、B、C、D），都会被透明模式防火墙获取（假设所有的计算机都在使用中）。

❑ 转发和过滤

在链路层，透明模式防火墙根据查找地址表成功后转发处理、查找地址表成功后不转发（过滤）处理和查找地址表失败后转发处理 3 种情况对数据帧作出转发或不转发（即过滤）处理。

若计算机 A 向计算机 C 发送以太网帧，透明模式防火墙通过查找地址表知道计算机 C 与端口 2 对应，则将该帧从端口 2 转发出去，即查找地址成功后转发处理数据情况。另外，当透明模式防火墙在某端口接收到广播帧或多播帧时，也将向其他端口进行转发，如图 9-15 所示。

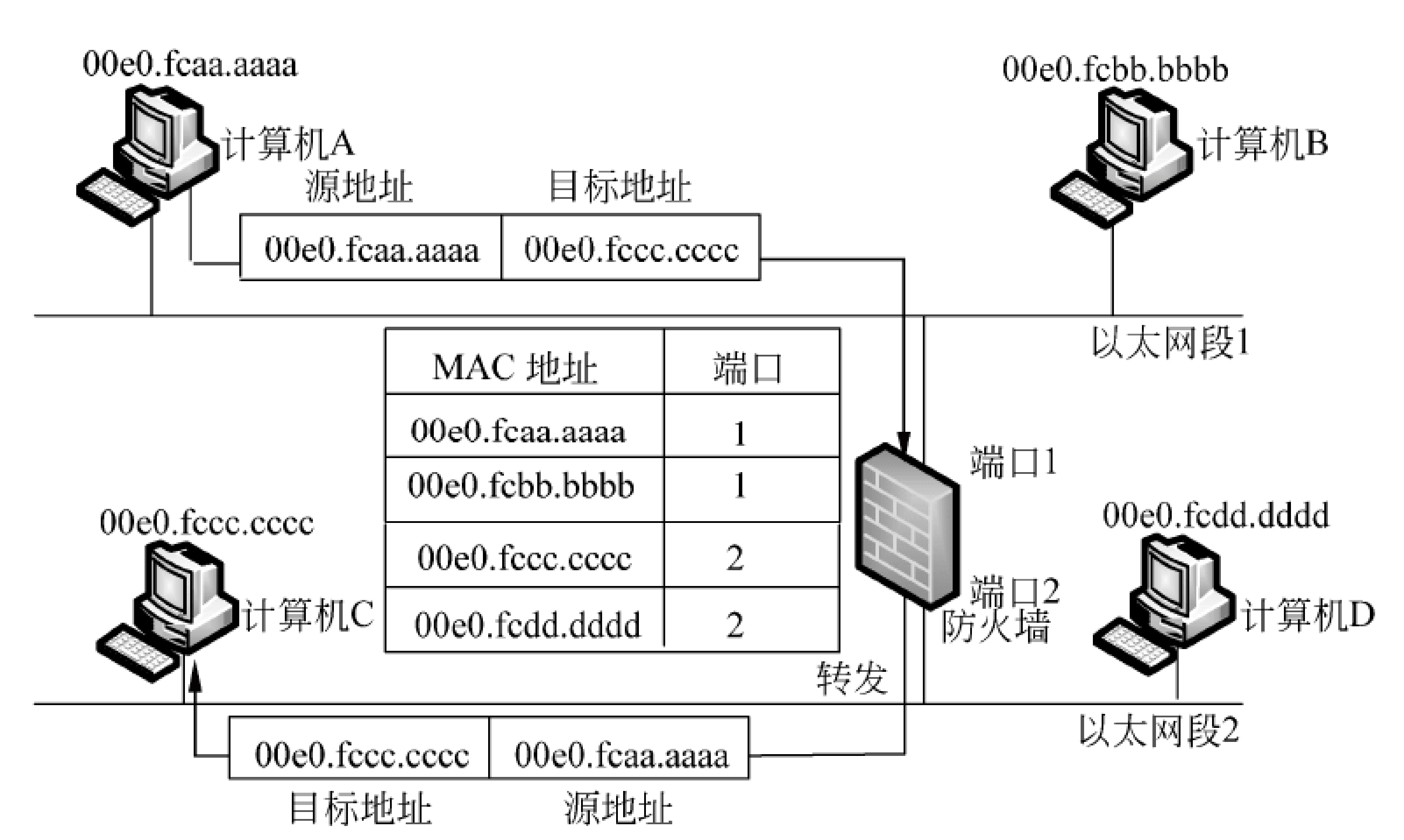


图 9-15　查找地址表成功后的转发处理

若计算机 A 向计算机 B 发送以太网帧，由于计算机 B 与计算机 A 在同一个物理网段上，透明模式防火墙对此帧进行过滤，不转发该帧，即查找地址表成功后数据不转发（过滤）处理，如图 9-16 所示。

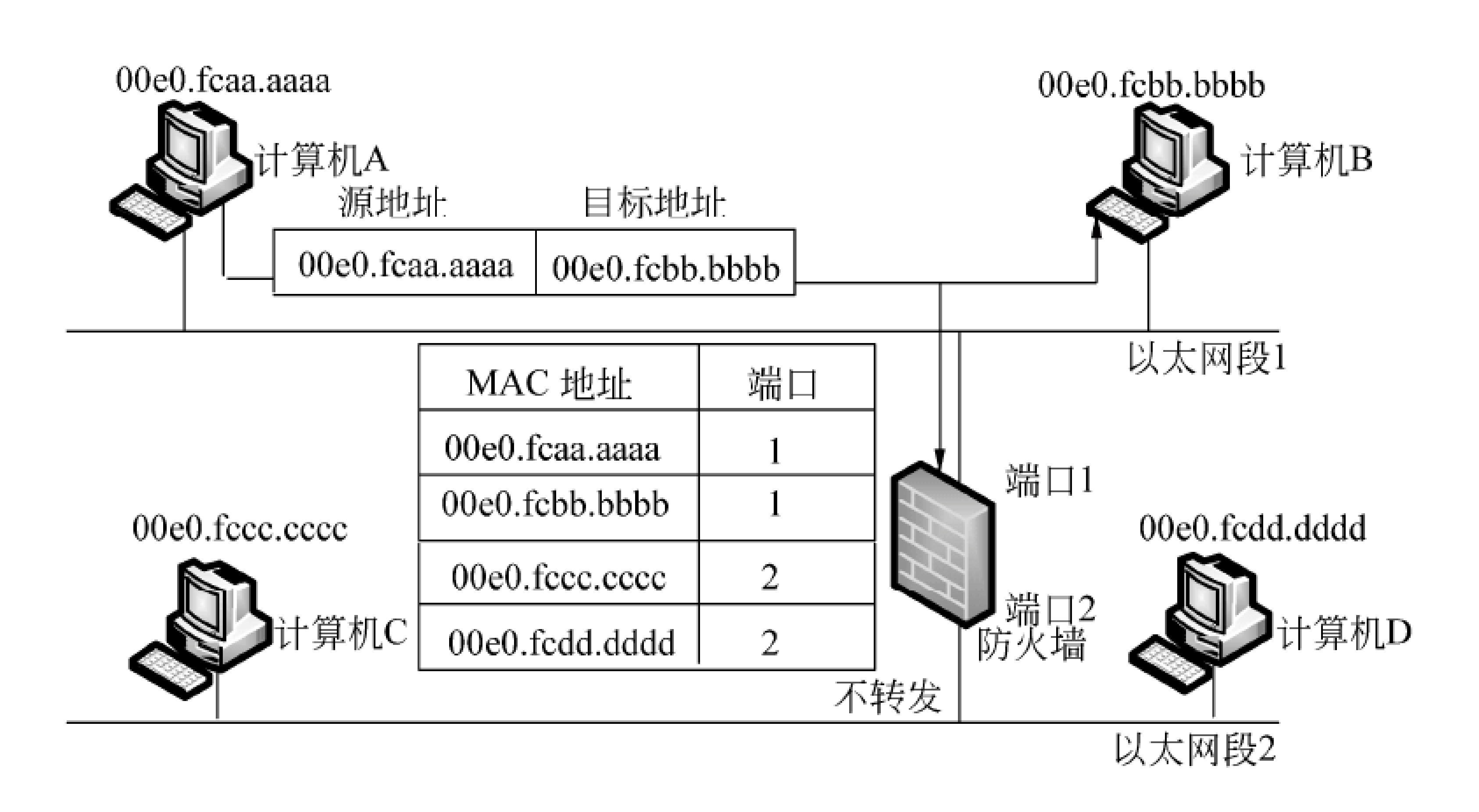


图 9-16　查找地址表成功后不转发（过滤）处理

若计算机 A 向计算机 C 发送以太网帧，而在地址表中未找到关于计算机 C 的 MAC 地址

与端口的对应关系，此时，透明模式防火墙会把这个发往未知目的 MAC 地址的帧向除发送该帧的源端口外的其他所有端口进行转发，如图 9-17 所示，这属于查找地址失败后转发处理情况。在这种情况下，透明模式防火墙充当的实际上是集线器角色，从而确保没有停止信息的传送。

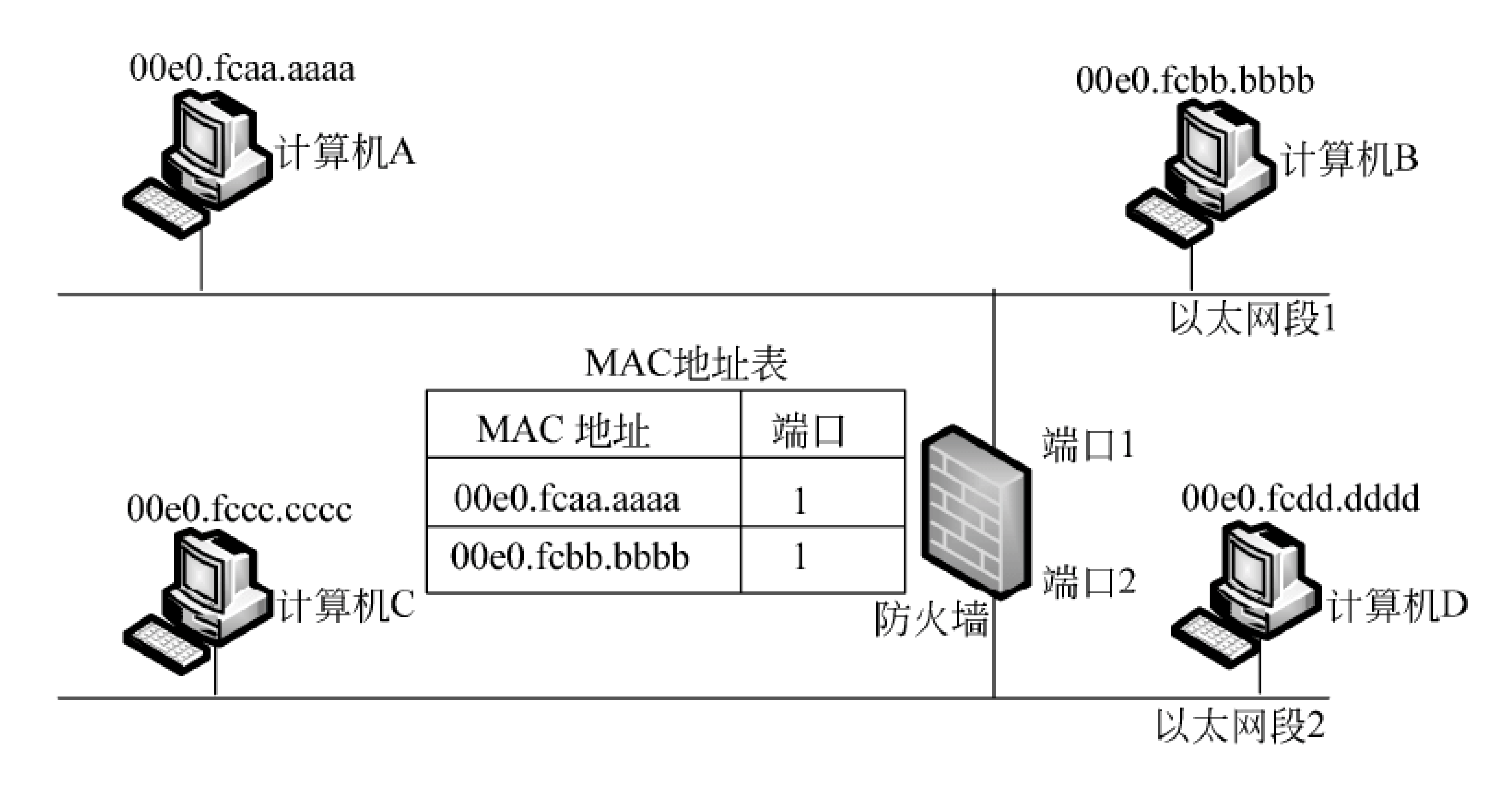


图 9-17　查找地址失败后转发处理

5. 混合模式

若防火墙既存在工作在路由模式的接口（接口具有 IP 地址），又存在工作在透明模式的接口（接口无 IP 地址），则称防火墙工作在混合模式下。

混合模式主要用于透明模式作双机备份的情况，此时启动 vrrp（virtual router redundancy protocol，虚拟路由冗余协议）功能的接口需要配置 IP 地址，其他接口不配置 IP 地址。防火墙混合模式的典型组网方式如图 9-18 所示。

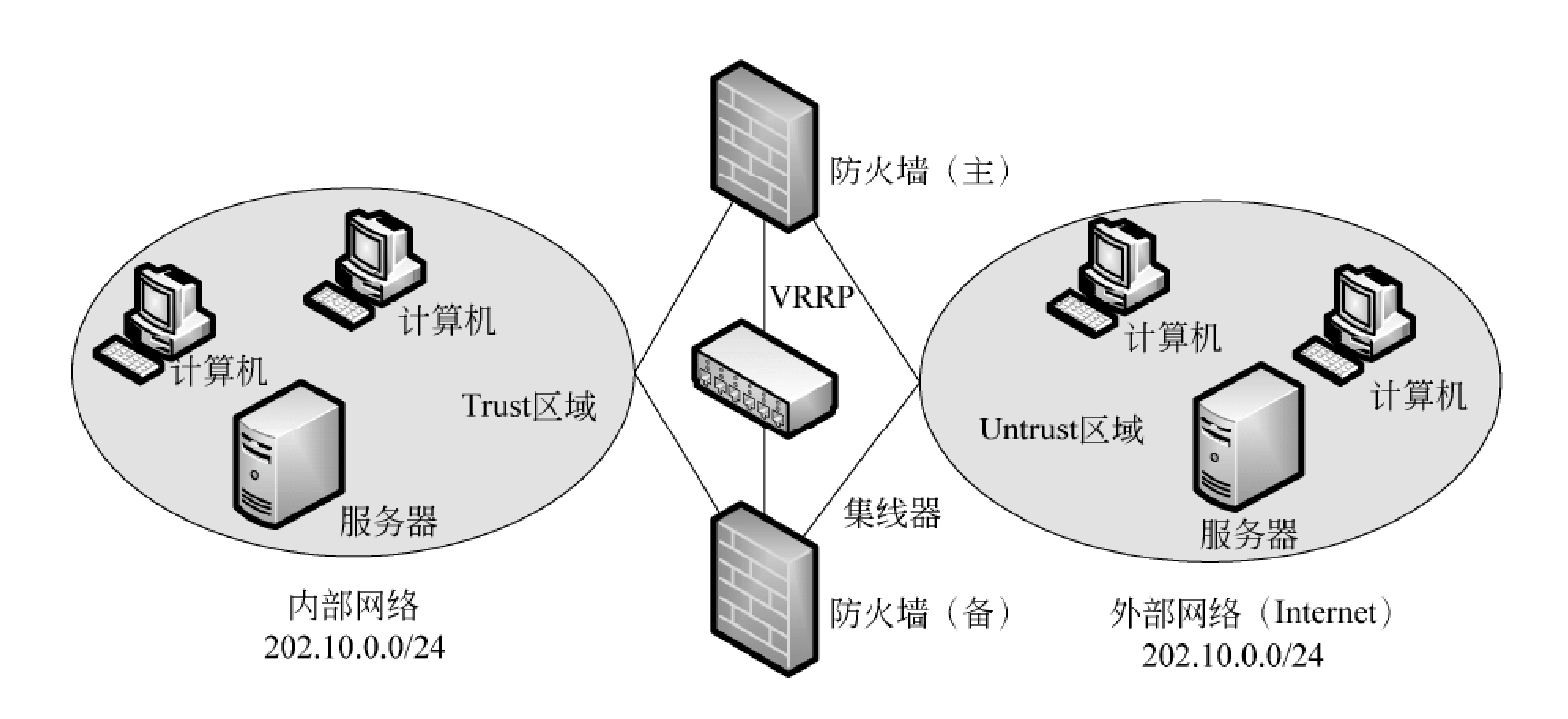


图 9-18　混合模式组网图

如图 9-18 所示，主/备防火墙的 Trust 区域接口与公司内部网络相连，Untrust 区域接口与外部网络相连，主/备防火墙之间通过集线器或局域网交换机实现互相连接，并运行 vrrp 协议

进行备份。需要注意的是内部网络和外部网络必须处于同一个子网。

6. 混合模式工作过程

防火墙工作在混合透明模式时，部分接口配置 IP 地址，部分接口不能配置 IP 地址。配置 IP 地址的接口所在的安全区域（三层区域），接口上启动 vrrp 功能，用于双机热备份；而未配置 IP 地址的接口所在的安全区域（二层区域），和二层区域相关接口连接的外部用户同属一个子网。

当报文在二层区域的接口间进行转发时，转发过程与透明模式的工作过程完全相同。当防火墙进行双机热备份时，转发过程类似路由模式的工作过程中的描述。

9.4.2 防火墙的配置规则

前面介绍了防火墙的规则，提到了“防火墙规则”(Firewall Rules)，规则是防火墙的思维，它们其实是一条条描述语句，用于设置防火墙行为等，每一条规则都对应了一种特定的行为判断，防火墙根据规则的内容对符合条件（端口、协议类型，甚至包数据）的数据包给予拦截或通行，当然也可以记录数据。正是由于这些众多的规则结合，防火墙才能给网络带来一个牢固而灵活的安全保护体系。

配置防火墙规则比较复杂，一个防火墙的工作效率、拦截放行、总体安全系数除了要求防火墙的引擎功能强大之外，关键在于防火墙规则的设置，如果防火墙引擎不能识别复杂的数据包结构，那么一些描述复杂的规则就不能正常工作，但一个防火墙越强大，其相应的规则设置也就越复杂，对于防火墙而言，一条好的规则就比什么都重要。

规则的设置，是围绕着一定的“安全策略”实施，许多防火墙产品在市场上出售时，已经存在默认规则，而这些规则就是厂商的“安全策略”的实体对象，许多用户安装或购买一个防火墙产品后，就一直没对这些规则做过修改，或者不知道防火墙规则的存在，但他们依然能得到防火墙的保护，正是因为厂商已经为这些防火墙套用了“兼容的”规则集合。

换句话说，用户在接受一款防火墙产品时，就已经得到了厂商定制的“安全策略”。但这种面对大众的策略并不一定适合每一个人。有时，一些用户会觉得默认规则不太适合自己的实际环境，他们便会根据自己的要求，修改增加这个规则集合。

例如，一台网站服务器，使用的防火墙默认规则里限制了外部对 1024 以下低端口号的访问，这和做网站需要开放 80 端口的要求相冲突，所以网络管理员将修改防火墙规则，去掉这条限制规则或者从规则里除掉 80 端口的条件，即防火墙“安全策略”实施的过程。

另外，在防火墙配置规则中，规则次序也是一个不可忽略的配置部分。因为大部分防火墙产品是按照顺序读取规则设置的，如果发现了一条匹配的规则，那么下面的其他规则描述则被忽略掉，所以规则的排列次序决定着防火墙的运作情况，管理员在配置规则时必须把属于特殊性质而又不容易与其他现存规则发生冲突的规则放到最前面，最大限度防止防火墙在找到一个特殊规则之前与普通规则相匹配，而导致管理员设置的安全规则失效。

前面已经提到，防火墙规则就是一条条用于描述防火墙在遇到什么类型的数据包时应该怎么做的命令语句，根据防火墙核心能识别的深度差异，不同防火墙的规则定义也不尽相同，但是基本上都离不开这几个基本参数：数据包方向、数据包地址、范围、协议类型、端口号、

标志位（TCP）、包类型和代码（ICMP）以及满足条件时的防火墙动作（通行、拦截、忽略、记录）等。

正是这些参数的各种搭配，才构筑了最终能够保护用户免遭网络攻击的一条条规则，成为用户的安全体系结构，一款防火墙产品核心能识别的数据类型越多，相应的规则设定就越复杂。因此，在进行防火墙规则设置时必须进行认真规划。

9.4.3　ISA Server 的应用

ISA Server 和目前广泛使用的其他防火墙存在许多不同，但最根本的区别是 ISA Server 结合了状态过滤（包过滤）和应用层状态识别，并且提供了 VPN 服务和 Web 代理/缓存服务，使其他防火墙和 ISA Server 相比显得有些低能。

ISA Server 的另一个关键组成则是它可以对通过它的任何连接进行身份验证。和传统的状态过滤防火墙相比，ISA Server 可以对任何通过它的 TCP 或 UDP 连接进行透明的身份验证。因此，不仅可以在外部（Internet）访问内部网络时加以保护，也可以在内部用户访问外部网络时进行基于用户/用户组的控制。

传统的防火墙管理员一般只是理解“开放端口”，而通过 ISA Server 提供的用户/用户组控制，ISA Server 管理员则可以监控到访问外部网络的用户和应用程序。这样，在需要对网络活动进行控制和分析报告时，可很容易做到。

1．ISA Server 访问规则的处理过程

为了从功能角度描述在被定义的网络间，何种通信是被允许的，ISA Server 使用了一组 3 个规则列表的集合。

- **网络规则**

该列表定义并描述了网络的拓扑结构。这些规则用于决定两个网络实体间是否具有路由关系及何种路由关系被定义（路由还是 NAT）。当网络实体间没有配置任何关系，那么 ISA Server 将丢弃两个网络间的所有通信数据。正确定义网络对象和它们之间的路由关系对于 ISA Server 显得非常重要。

- **系统策略**

该列表包含了 30 条 ISA Server 预定义的、应用于本地计算机的访问策略。所以，它们控制着 ISA Server 本身“从/到”的通信，并启用需要的诸如验证、网络诊断、日志和远程管理等功能。这些规则只是“允许”规则，只可以启用或禁用这些规则，或者对其中的一些规则属性进行少量的修改。

- **防火墙策略**

该列表包含了自定义的所有规则。这是一个经过排序的简单列表，涵盖了两种可能的规则类型，即访问规则和发布规则。在此列表的最后一条预定义的默认规则为 Deny 4 ALL（Deny ALL users use ALL protocols from ALL networks to ALL networks，拒绝所有用户发起的从所有网络到所有网络的所有协议的访问）。这个默认规则不能修改或删除，所以对于任何允许或者阻止的通信都有 ISA Server 的一条明确规则完成。

对于所有的访问请求，ISA Server 如何应用上述 3 条规则列表如图 9-19 所示。

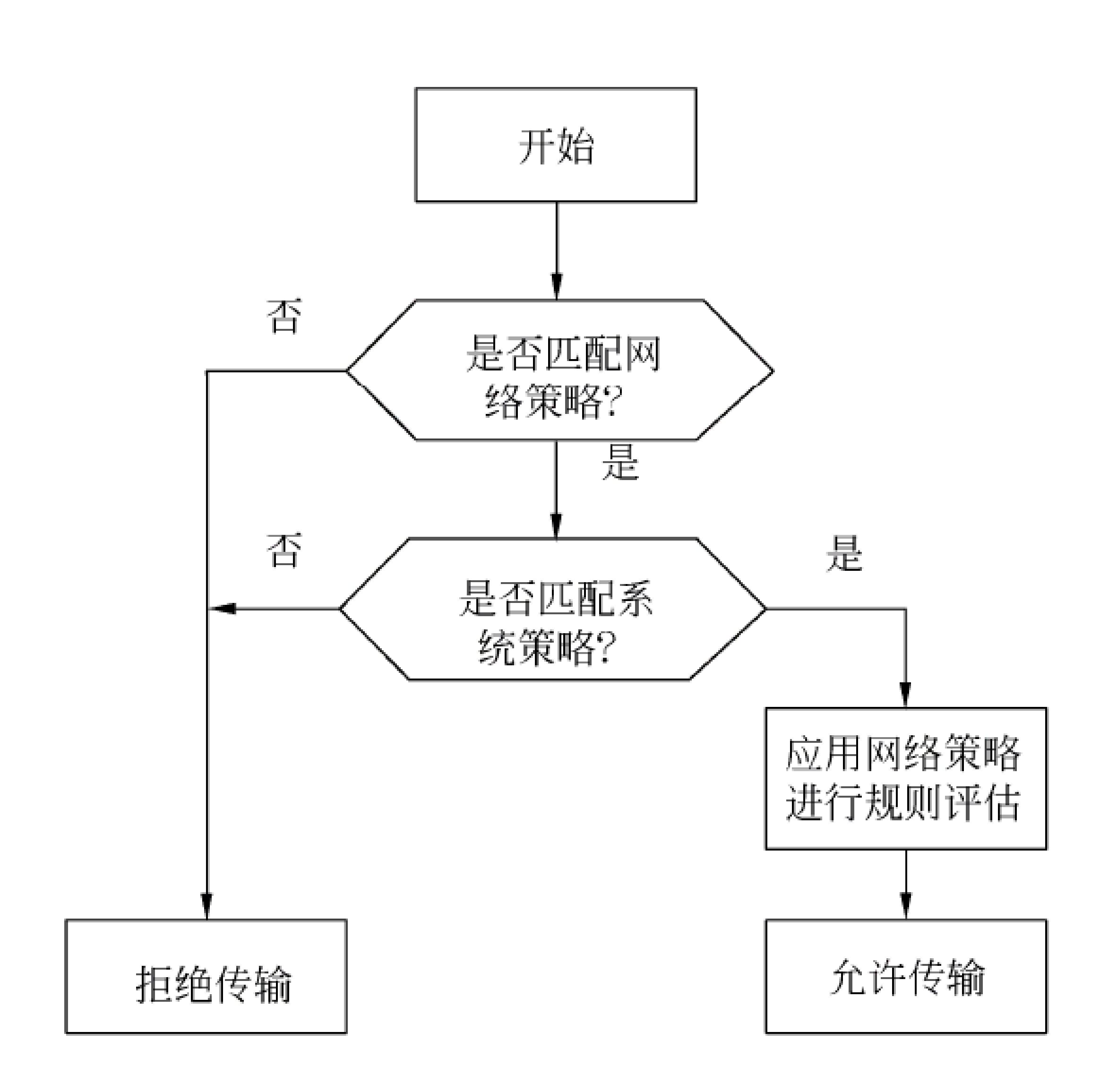


图 9-19　ISA Server 规则的处理

首先，ISA Server 检查网络规则以确定两个网络实体间是否定义了路由关系，如果源网络和目标网络之间定义了路由关系，那么 ISA Server 将进一步处理客户的出站请求，否则拒绝。

然后，ISA Server 按顺序检查系统策略规则和防火墙策略规则。如果某个系统或者防火墙策略规则允许了此请求，则 ISA Server 将进一步处理出站请求，否则拒绝。

最后，ISA Server 再次检查网络规则以确定数据包的路由方式是路由还是 NAT，如果是 Web Proxy 客户端请求对象，ISA Server 将会检查 Web 连接规则，以确定请求如何被处理。

很明显，网络规则处理的逻辑非常简单明了，即是否定义了两个网络实体间的路由关系。但对于 ISA Server 如何确定一个系统策略或防火墙策略的规则，允许或拒绝此通信却并非那么简单。在此，所了解的只有系统策略优先于防火墙策略进行处理，即 ISA Server 对系统策略和防火墙策略的处理的方式是一致的。

2. 防火墙策略

ISA Server 主要控制源网络和目标网络之间的通信，且源计算机和目标计算机必须位于不同的网络中。也就是说，不能通过 ISA Server 循环访问与其在同一网段的资源（虽然这样可以实现，但会给 ISA Server 带来很大的性能负担）。

另外，ISA Server 严格按照顺序评估防火墙策略。如果一条访问规则匹配某个请求的参数，则此规则将被应用，然后 ISA Server 不再将此请求与其他任何规则进行匹配。

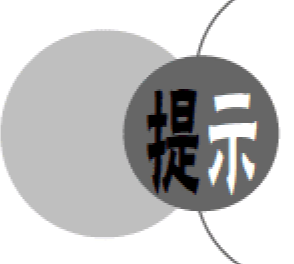
还需要记住的是系统策略优先于防火墙策略进行处理，且 ISA Server 对系统策略和防火墙策略的处理方式是一致的。即一个完整的防火墙策略系统，可被认为是一个单一排序的序号从 1 到 30 的系统策略规则，加上从序号 31 开始的防火墙策略规则及最后的默认规则的列表。因此，如果一条系统策略规则和一条防火墙策略规则同时匹配某个客户发起的请求，那么总是会应用系统策略规则。

需要注意的是，访问规则是按照出站方向的主要连接端口来进行处理，所以在创建访问规则时，不能使用入站方向的协议。

在进一步讨论规则前，有必要先总结一下几种 ISA 客户端类型的不同点。表 9-1 总结了 3 种 ISA 客户端是如何发送请求及是否支持身份认证。

表 9-1 ISA 客户端类型及对应的请求、认证信息

ISA 客户端类型	如何发送请求	是否支持身份认证
Web 代理客户	根据用户的输入使用 TQDN（完全合格域名）或 IP 地址（提示）	支持（HTTP/HTTPS/封装 FTP）
防火墙客户	总使用 IP 地址（提示）	支持（所有基于 TCP/UDP 的协议）
SNAT 客户	总使用 IP 地址	不支持



对于所有的非 HTTP/HTTPS 请求来说是正确的，对于 HTTP/HTTPS 请求，ISA Server 总是检查 HTTP 头中的计算机字段，而不是请求的目标计算机地址（网络层地址）。对于 Web 代理客户，HTTP 主机头的值依赖于用户的输入

3. 匹配标准

现有的问题在于，客户的访问请求怎样才能匹配访问规则中定义的策略元素。如果请求匹配访问规则的策略元素，ISA Server 则运行此规则处理客户的访问请求。检查规则的顺序为协议、从（源网络）、计划时间、到（目标网络）、用户、内容类型，如表 9-2 所示。

表 9-2 ISA Server 匹配访问规则的策略元素及含义

策略元素	含义
协议	访问规则中为出站方向定义的主要连接端口范围，可以是一个或多个协议
从（源网络）	发起连接的一个或更多的网络对象，可以包含网络、网络集、计算机、计算机集、地址范围或子网
计划时间	定义的任何计划时间
到（目标网络）	连接到一个或更多的目标网络，可以包含网络、网络集、计算机、计算机集、地址范围、子网、域名集或 URL 集
用户	一个或更多的用户对象，可以包含所有用户、所有经过认证的用户、系统和网络服务和其他定义的用户集
内容类型	定义的任何内容类型

表 9-2 的一些元素很好理解，如协议、从（源网络）和计划时间，对于它们很容易区分是否匹配。但对于到（目标网络）、用户集、和内容类型这 3 个条件，则不是那么容易理解的。例如，在一条访问规则要求认证，而客户端发起的请求不能通过认证时，ISA Server 会对该请求采取怎样的处理方式呢？或在一条允许指定 URL/内容类型且包含 HTTP/HTTPS 协议的访问规则中，ISA Server 怎样处理？需要对其进行进一步阐述。

❑ **URL 集**

当在策略元素的到（目标网络）中，指定 URL 集，然后访问规则的协议中包含非 Web 协议（或 HTTP、HTTPS、封装 FTP 协议），ISA Server 会怎样处理？

在 ISA Server 处理到（目标网络）包含有 URL 集规则时，规则到（目标网络）中的 URL 集只对 Web 协议（HTTP、HTTPS、封装 FTP 协议）有效，但对于 HTTPS 传输，URL 集只有

在没有指定路径时进行匹配。如果客户使用其他协议进行访问，那么 ISA Server 将会忽略规则中的 URL 元素集。

为了进行验证，可修改防火墙策略，修改后的防火墙策略如表 9-3 所示。

表 9-3　修改后的防火墙策略

序号	协议	从	计划时间	到	用户集	内容类型	动作
1	FTP、HTTP	内部	Always	URLs	所有用户	全部	允许
2	FTP、HTTP	内部	Always	IPs	所有用户	全部	允许
Last	ALL	ALL	Always	ALL	ALL Users	ALL	Deny

此时，若使用 FTP（非封装的 FTP）访问www.cevi.be和www.pouseele.be 时，可看到客户请求是被规则 2允许，而不能匹配规则 1。

从另一方面说，当 ISA Server 为非 Web 协议的访问忽略了访问规则中的 URL 集，且在访问规则的到（目标网络）中未指定其他值时，ISA 将不能匹配这条规则，即这条规则将永远不会执行，而不管它是被允许还是拒绝。如果在规则 1 的目标网络中，添加 FQDN（www.cevi.be）后再进行策略，此时可发现到达 www.cevi.be 的 FTP 访问将被规则 1 允许，而到达 www.pouseele.be 的 FTP 访问将被规则 2 允许。

❑ 用户集

当建立防火墙策略后，可将它们应用到指定用户的 IP 地址或用户集。在指定用户集时，此用户必须进行验证，出示他的验证信息，然后 ISA Server 对规则进行匹配。用户集可包含任何认证方式的一个或多个用户。例如，一个用户集可包含 Windows 用户、Radius 用户和 SecurID 用户。ISA Server 预定义了如表 9-4 所示的用户集。

表 9-4　ISA 预定义的用户集

用户集	含义
所有经过认证的用户	表示为所有通过验证的用户，注意 Snat 客户端将不会进行认证，除非它们为 VPN 客户
所有用户	表示为所有用户，不论是否通过身份验证
系统和网络服务	表示 ISA 计算机上的本地系统和网络服务账户，将被 ISA Server 用于部分系统策略

另外，客户端如何进行认证取决于客户端的类型。利用防火墙客户进行会话建立时，ISA Server 要求客户进行身份验证，因此当防火墙客户后来再进行访问时，ISA 不会再询问客户端的身份验证信息，因为会话已经被验证过了。

若为 Web 代理客户时，在允许其访问后，可以配置 Web 代理客户的身份验证。如果在 Web 代理侦听器的属性中选择要求所有用户进行验证，则 ISA Server 将总是在检查防火墙策略之前要求用户提供身份验证信息，否则 ISA Server 只会在访问规则要求时才要求客户进行身份验证。同样可通过配置防火墙策略来进行验证，建立的防火墙策略如表 9-5 所示。

表 9-5　针对用户集创建的防火墙策略

序号	协议	从	计划时间	到	用户集	内容类型	动作
1	FTP、HTTP	内部	Always	外部	Tom	ALL	允许
2	FTP、HTTP	内部	Always	外部	所有经过认证的用户	ALL	允许
Last	ALL	ALL	Always	ALL	ALL Users	ALL	Deny

对于 Web 代理客户和防火墙客户的访问请求，结果为，通过规则 1，用户 Tom 允许使用 HTTP 和 FTP 访问任何站点。通过规则 2，其他经过认证的用户可使用 HTTP 和 FTP 访问任何站点；在 ISA Server 进行策略的评估时，虽然其他用户也提交了身份验证信息，但不匹配规则 1 的用户集，所以 ISA Server 将跳过规则 1 检查下一条规则，然后发现完全匹配规则 2，就按照规则中定义的动作来允许客户的访问。

对于非 VPN 客户的 Snat 用户，结果为，在规则 1 就拒绝了匿名用户的 HTTP 和 FTP 访问；当 ISA Server 对规则 1 进行评估时，将发现客户发起的连接请求匹配规则 1 的协议、从（源网络）、计划时间、到（目标网络）元素，所以会要求客户提交身份验证信息，但 Snat 客户不能提交身份验证信息，此时 ISA 则会立即丢弃客户发起请求，也不会再进行下一条规则的评估。

9.5　操作实例

9.5.1　操作实例——ISA 的构建与配置

ISA 2004 是微软公司推出的一款网络安全产品，ISA 具有灵活的多网络支持、易于使用且高度集成的 VPN 配置、可扩展的用户身份验证模型、深层次的 HTTP 过滤功能，被公认为 X86 架构下最优秀的企业级路由软件防火墙。

1. 实例目的

- 创建新 ISA 服务器企业。
- 安装 ISA 服务器服务。
- 安装 ISA 配置存储服务器。
- 创建 Web 代理客户端。

2. 实例步骤

（1）在【Microsoft ISA Server 2004 安装程序】主界面中，单击【安装 ISA Server 2004】按钮，如图 9-20 所示，然后在弹出的【欢迎使用 Microsoft ISA Server 2004 安装向导】对话框中，单击【下一步】按钮。

（2）在【许可协议】对话框中，选中【我接受许可协议中的条款】单选按钮，并单击【下一步】按钮，如图 9-21 所示。

（3）在【客户信息】对话框中，输入用户名和密码，如“mytext”，并单击【下一步】按钮，如图 9-22 所示。

（4）在【安装方案】对话框中，选中【同时安装 ISA 服务器服务和配置存储服务器】单选按钮，并单击【下一步】按钮，如图 9-23 所示。

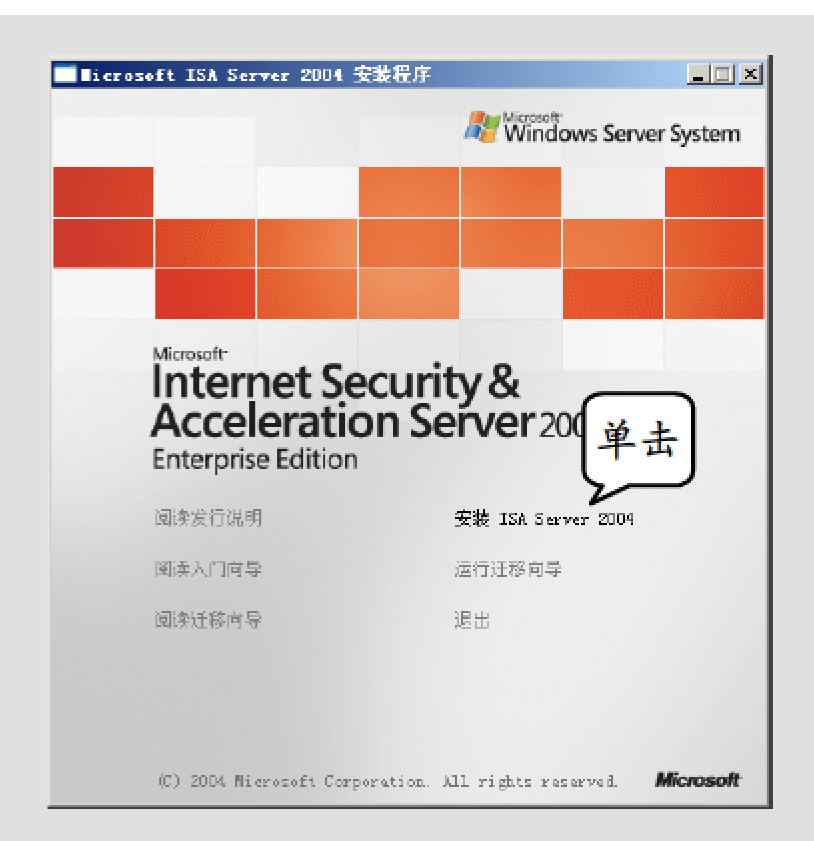


图 9-20　ISA Server 2004 主界面

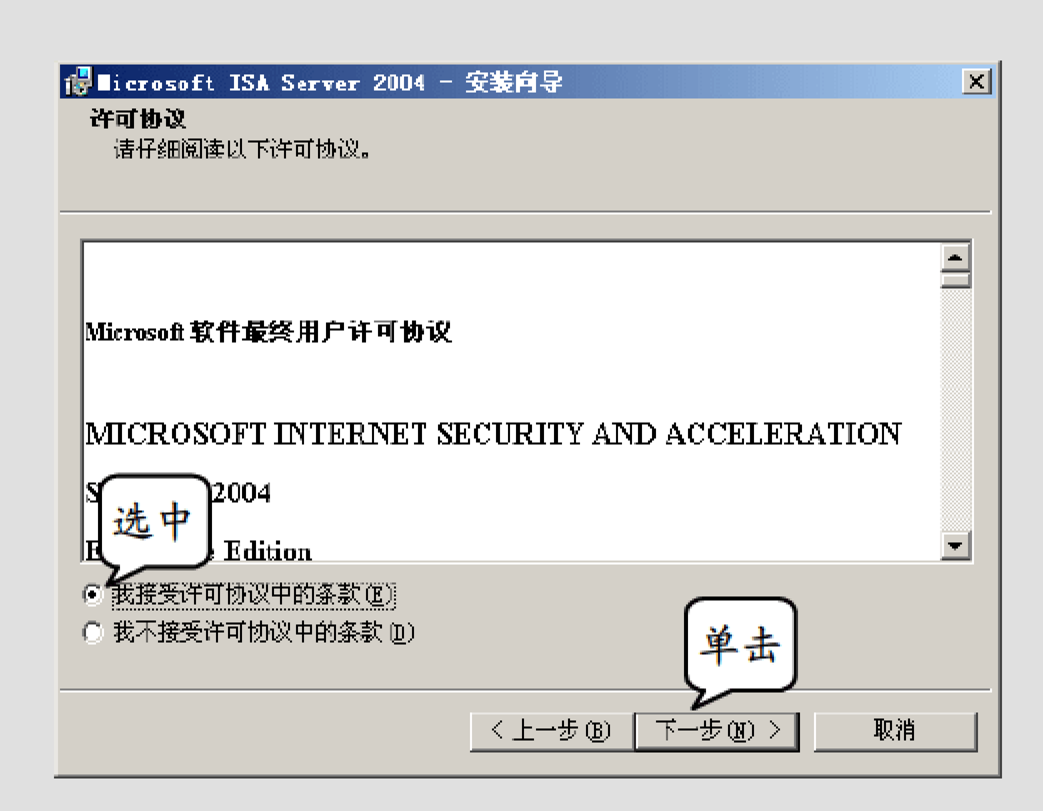


图 9-21　【许可协议】对话框

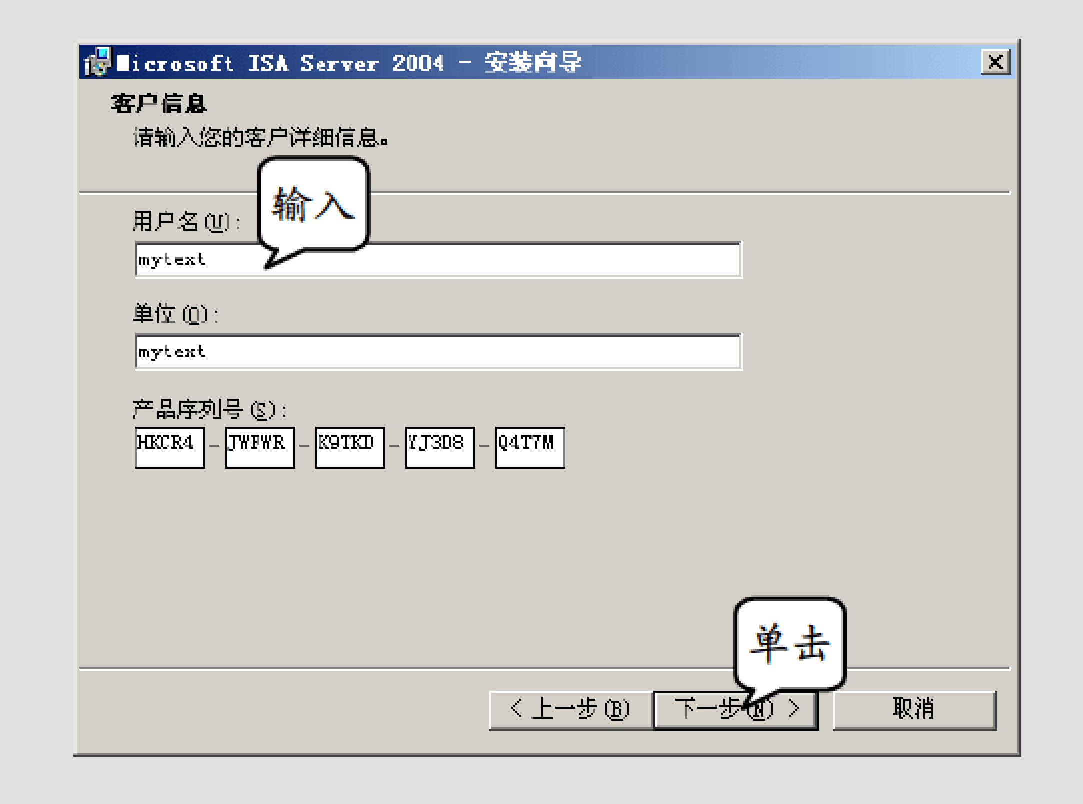


图 9-22　【客户信息】对话框

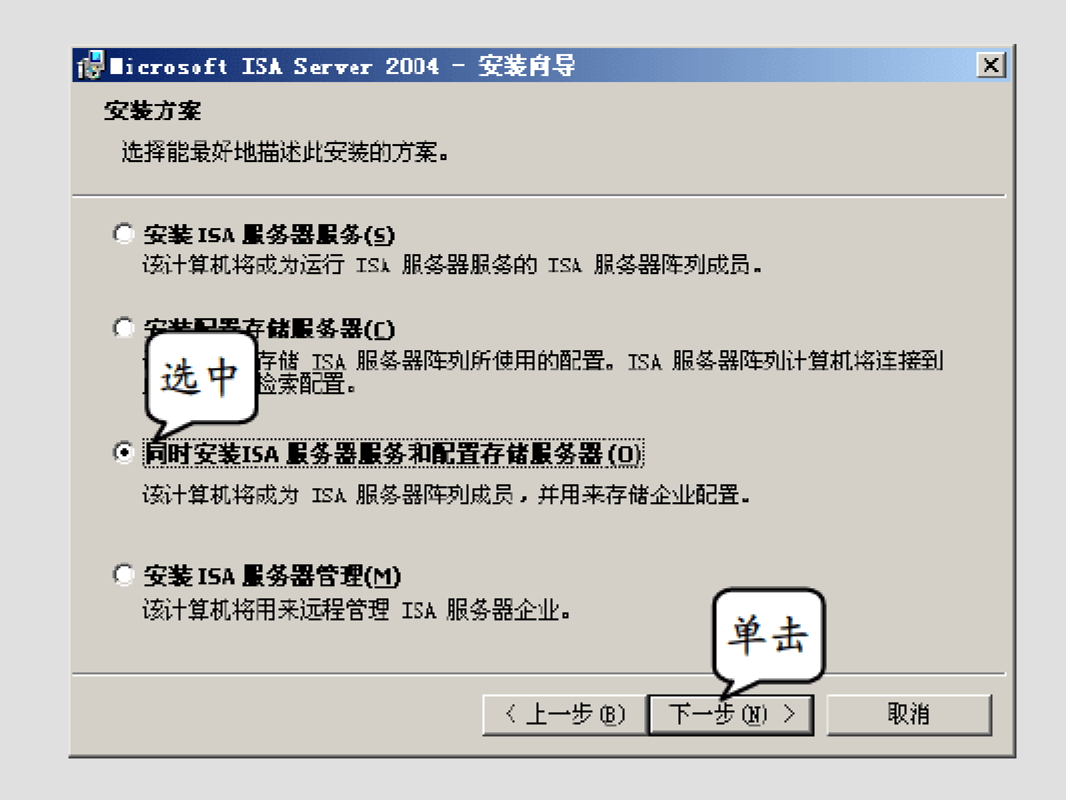


图 9-23　【安装方案】对话框

（5）在【组件选择】对话框中，单击【下一步】按钮，如图 9-24 所示。

（6）在【企业安装选项】对话框中，选中【创建新 ISA 服务器企业】单选按钮，并单击【下一步】按钮，如图 9-25 所示，然后在【新企业警告】对话框中，单击【下一步】按钮。

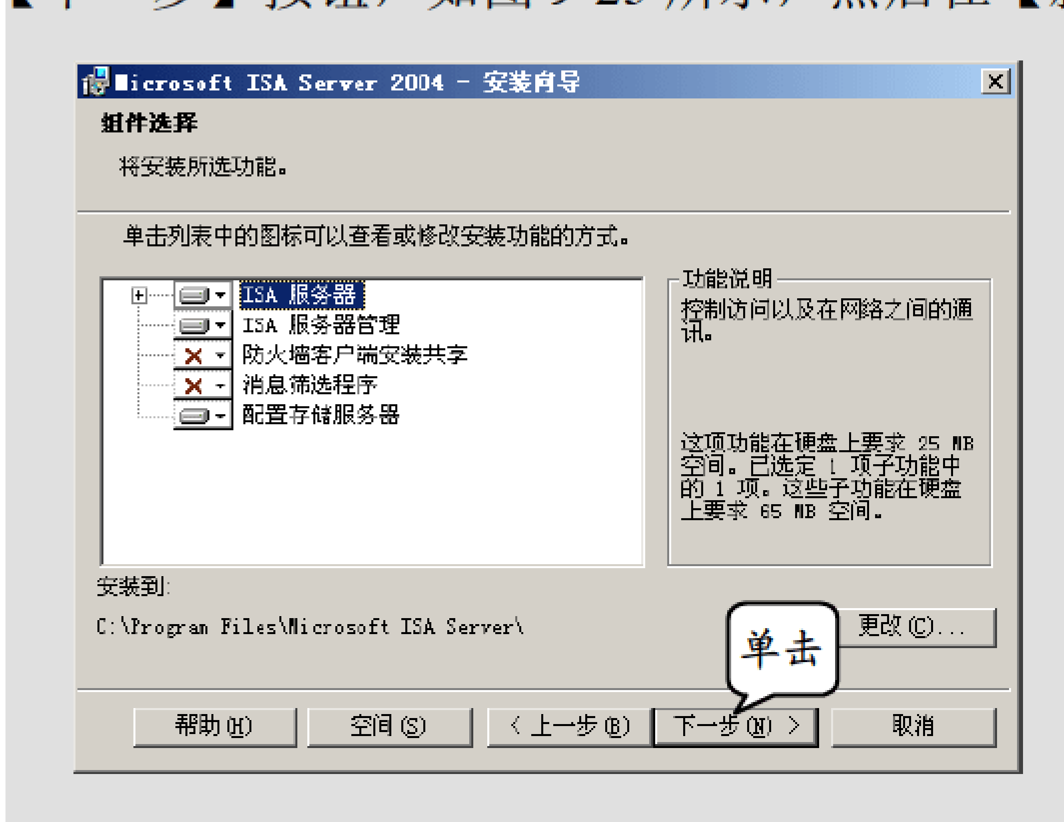


图 9-24　【组件选择】对话框

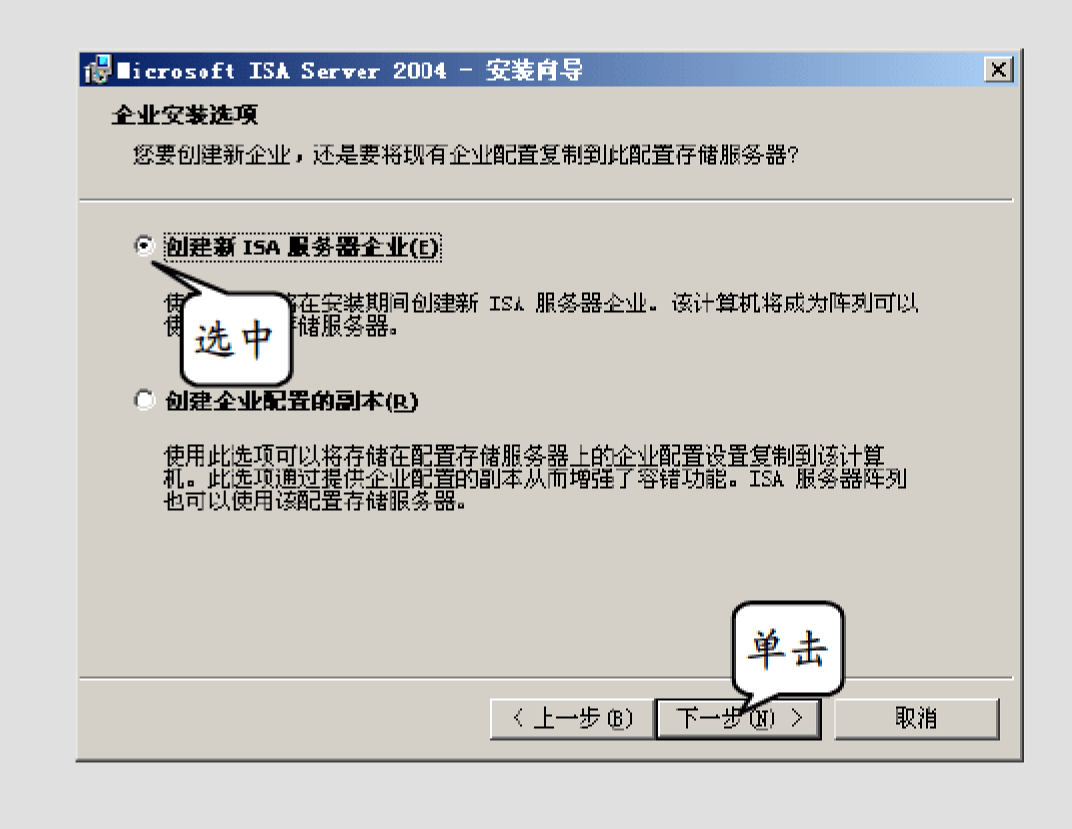


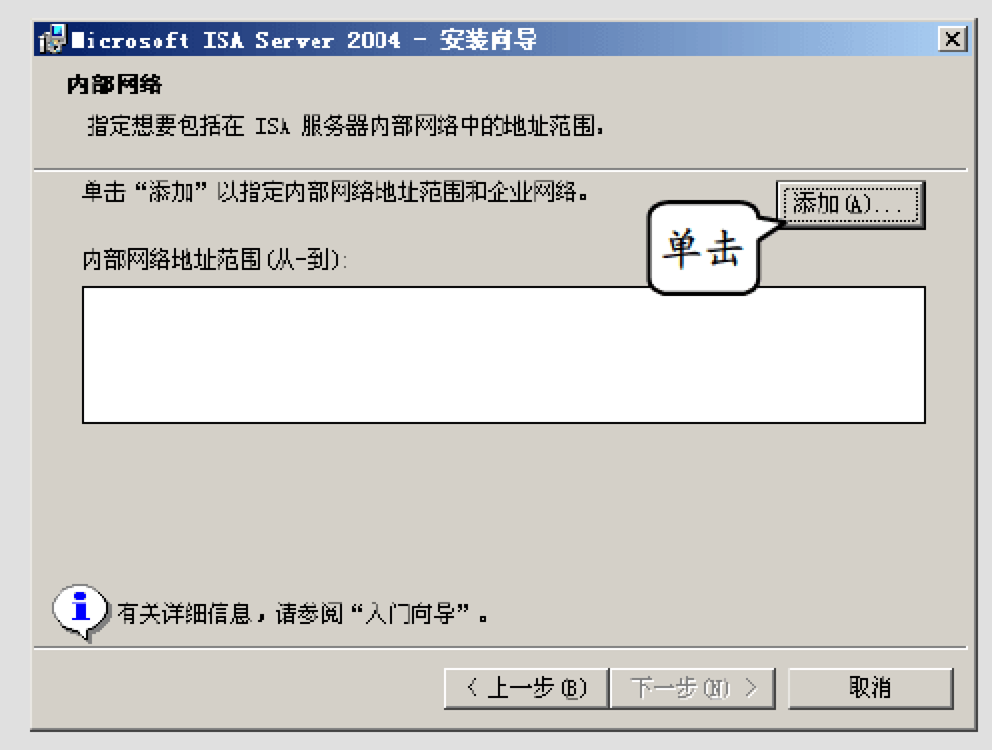
图 9-25　【企业安装选项】对话框

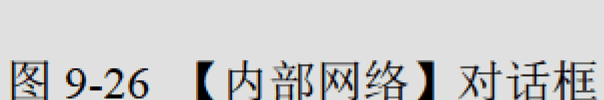
（7）在【内部网络】对话框中，单击【添加】按钮，如图 9-26 所示。

（8）在【地址】对话框中，单击【添加范围】按钮，如图 9-27 所示。

（9）在弹出的【IP 地址范围属性】对话框中，分别输入起始地址“10.1.1.6”和结束地址

“10.1.1.254”，并单击【确定】按钮，如图 9-28 所示。





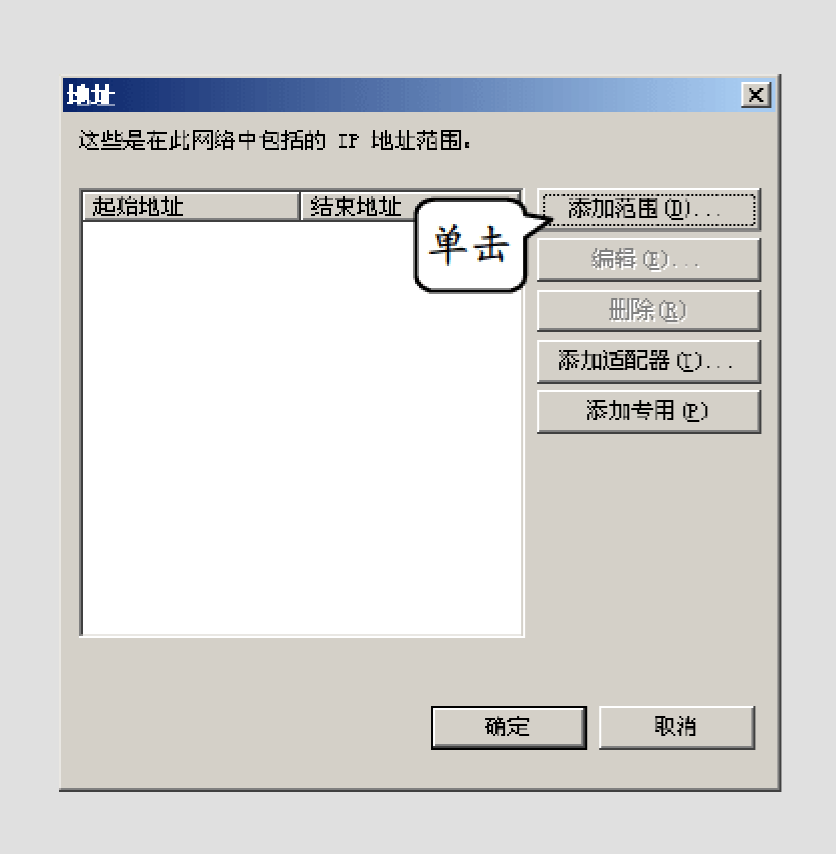
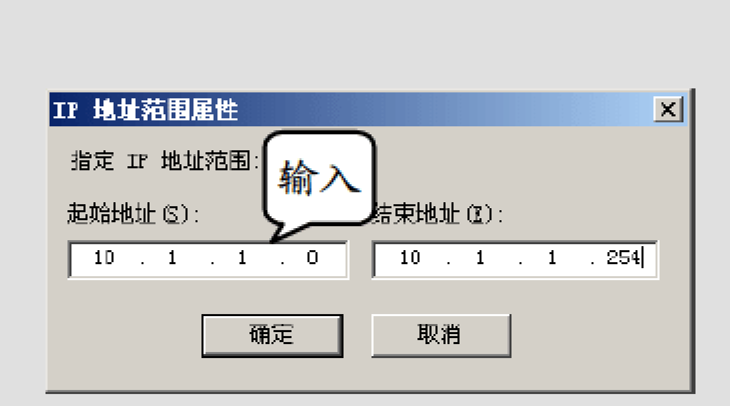


图 9-26 【内部网络】对话框　　　　图 9-27 【地址】对话框

（10）在返回的【地址】对话框中，单击【确定】按钮，如图 9-29 所示，并在【内部网络】对话框中，单击【下一步】按钮。



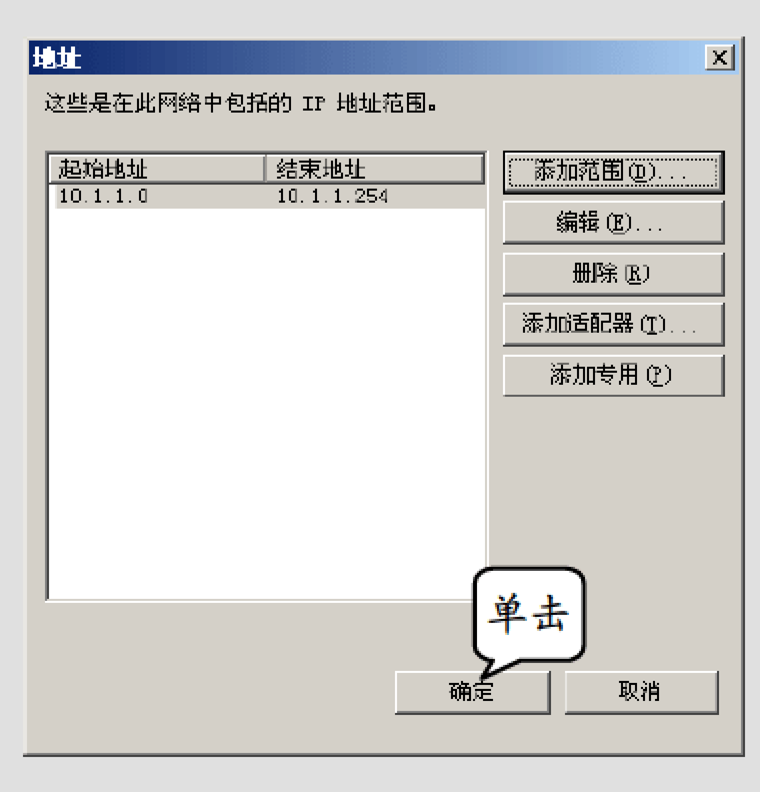
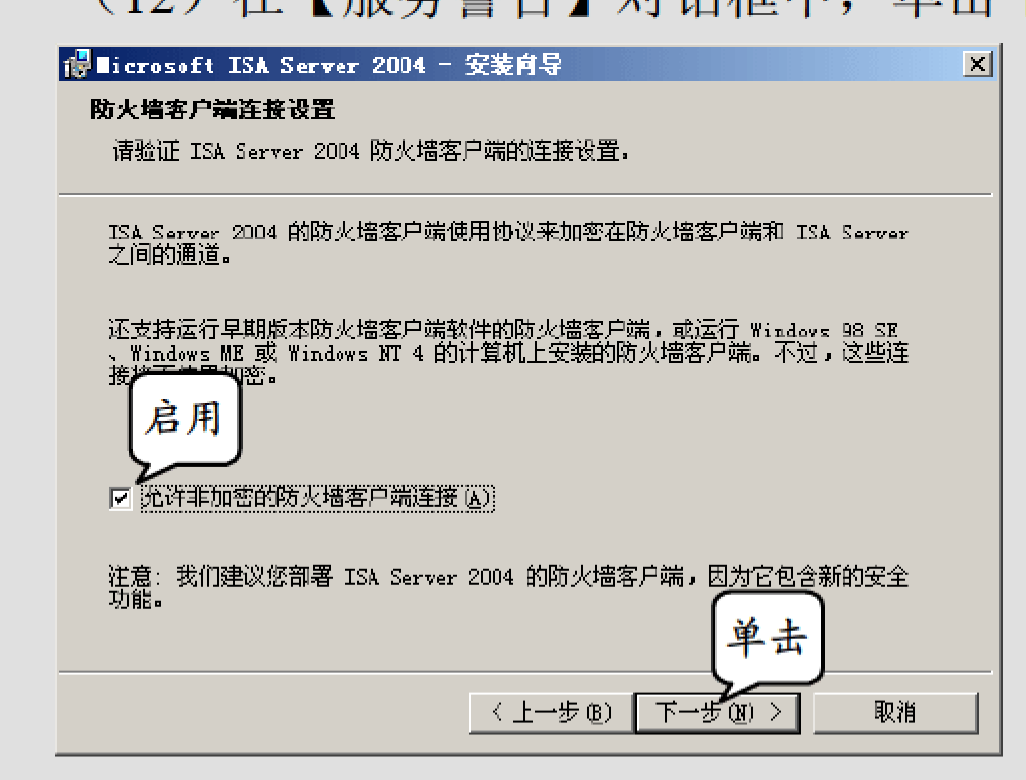


图 9-28　输入 IP 地址范围　　　　图 9-29 【地址】对话框

（11）在【防火墙客户端连接设置】对话框中，启用【允许非加密的防火墙客户端连接】复选框，并单击【下一步】按钮，如图 9-30 所示。

（12）在【服务警告】对话框中，单击【下一步】按钮，如图 9-31 所示。



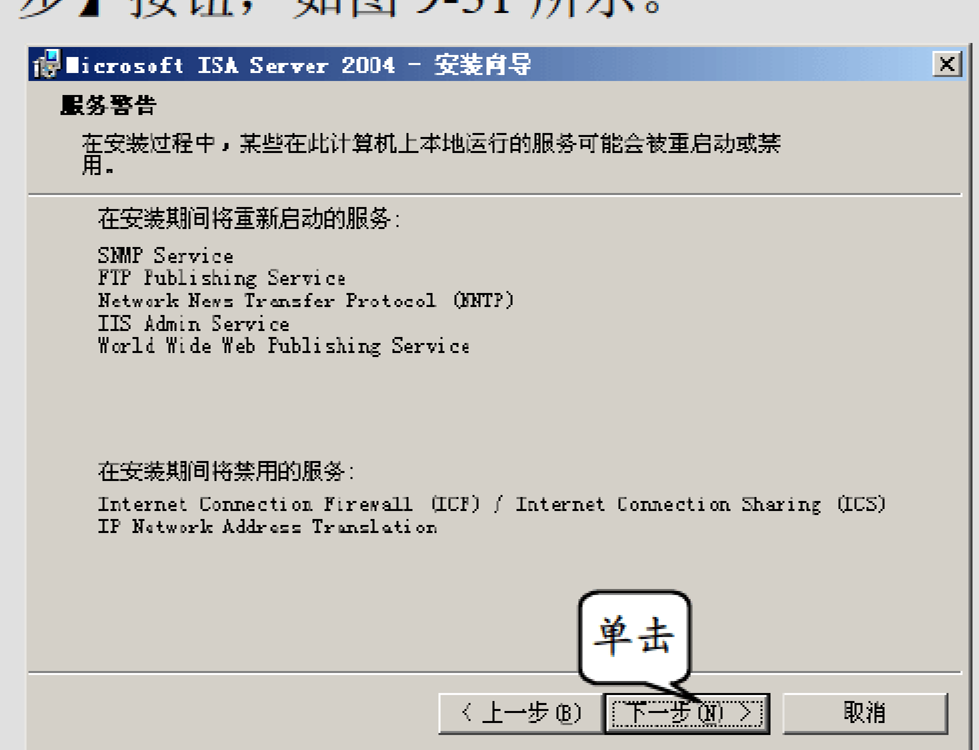
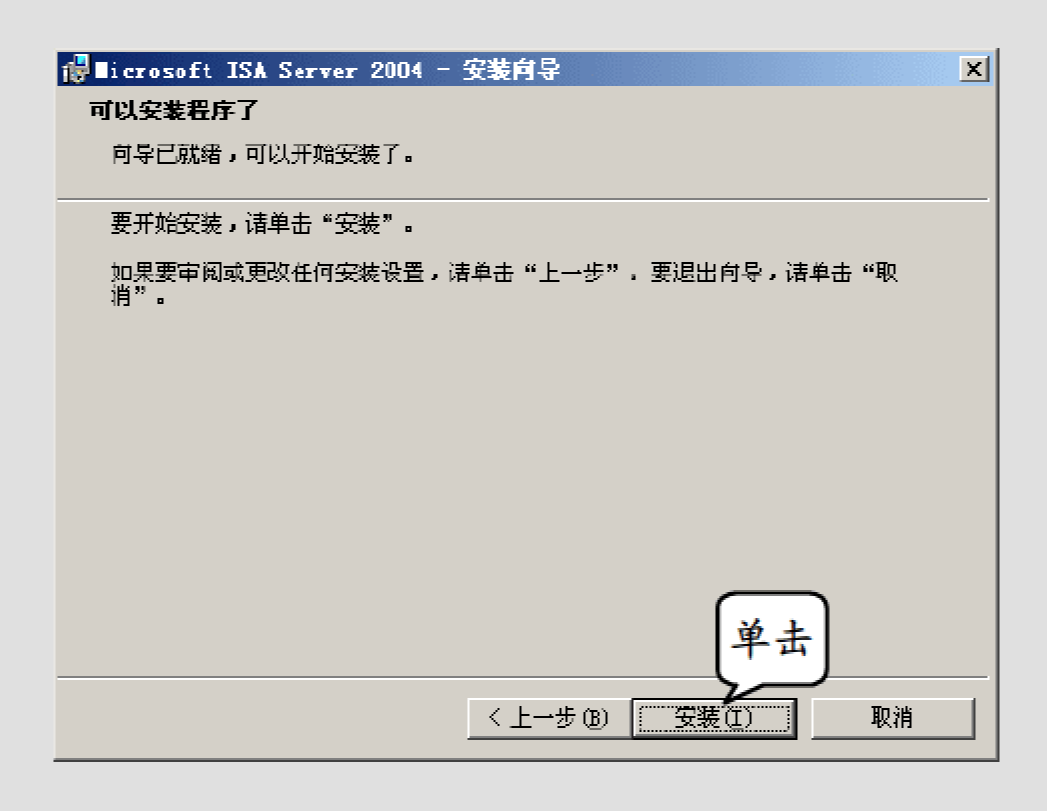


图 9-30 【防火墙客户端连接设置】对话框　　　　图 9-31 【服务警告】对话框

（13）在【可以安装程序了】对话框中，单击【安装】按钮，如图 9-32 所示。

（14）在【安装向导完成】对话框中，单击【完成】按钮，如图 9-33 所示。



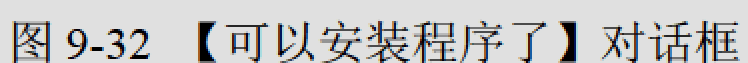


图 9-32 【可以安装程序了】对话框

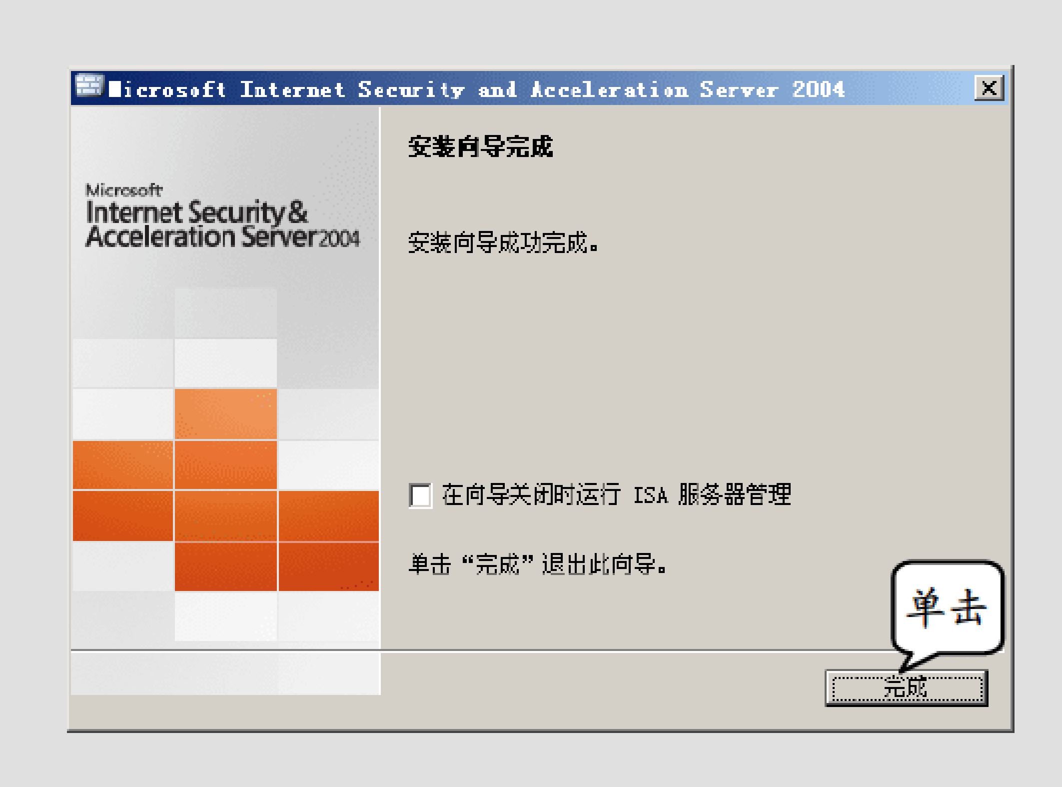


图 9-33 【安装向导完成】对话框

（15）内网客户计算机 IP 地址为"10.1.1.6"，ISA 内部接口地址为"10.1.1.254"，ISA 外部接口地址为"192.168.0.2"，实验环境，如图 9-34 所示。

（16）执行【开始】|【程序】|Microsoft ISA Server|【ISA 服务管理器】命令，在打开的窗口中，展开【阵列】节点，并双击 MYTEXT 选项，如图 9-35 所示。

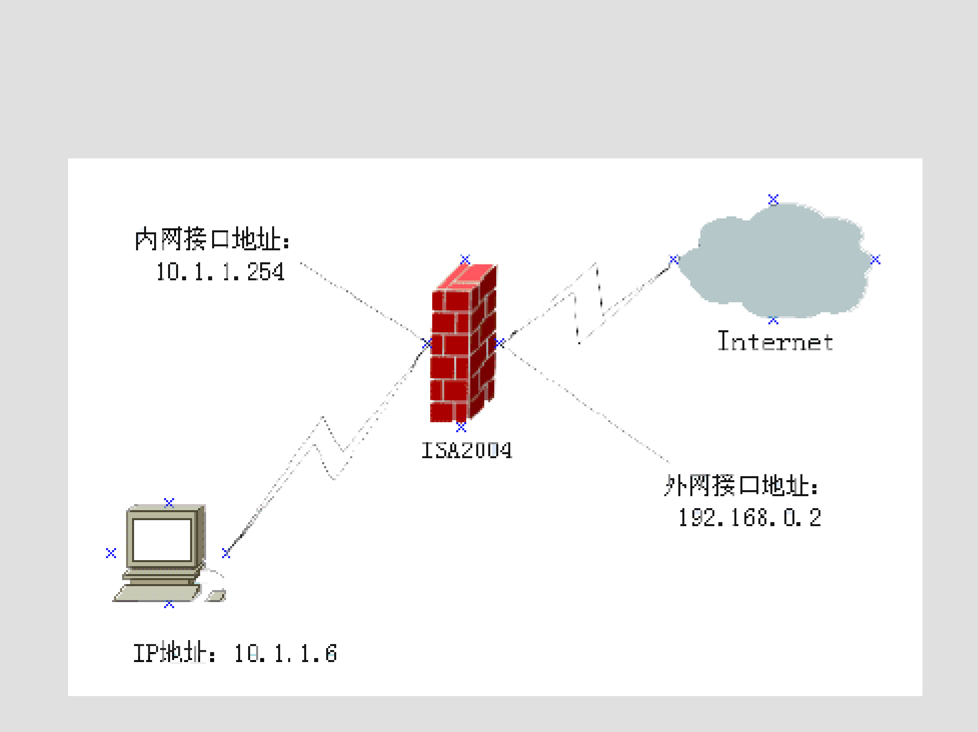


图 9-34 实验拓扑图



图 9-35 展开【阵列】节点

（17）右击【防火墙策略】选项，执行【新建】|【访问规则】命令，如图 9-36 所示。

（18）在弹出的【欢迎使用新建访问规则向导】对话框中，输入访问规则名称，如"允许内网用户任意访问"，并单击【下一步】按钮，如图 9-37 所示。

（19）在【规则操作】对话框中，选中【允许】单选按钮，并单击【下一步】按钮，如图 9-38 所示。

（20）在【协议】对话框中，单击【此规则应用到】下拉按钮，并选择【所有出站通讯】选项，然后单击【下一步】按钮，如图 9-39 所示。

（21）在【访问规则源】对话框中，单击【添加】按钮，如图 9-40 所示。

（22）在弹出的【添加网络实体】对话框中，双击【网络】选项，选择【内部】选项，然后依次单击【添加】和【关闭】按钮，如图 9-41 所示。

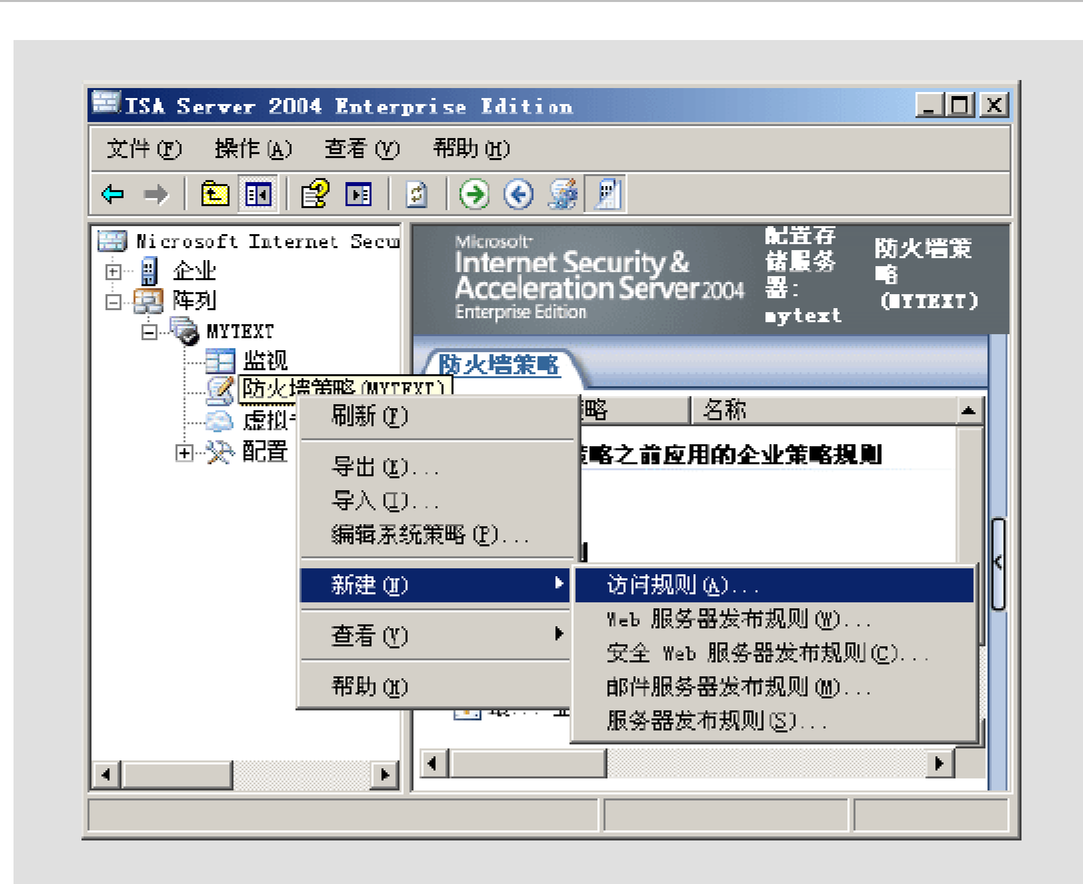


图 9-36　新建访问规则

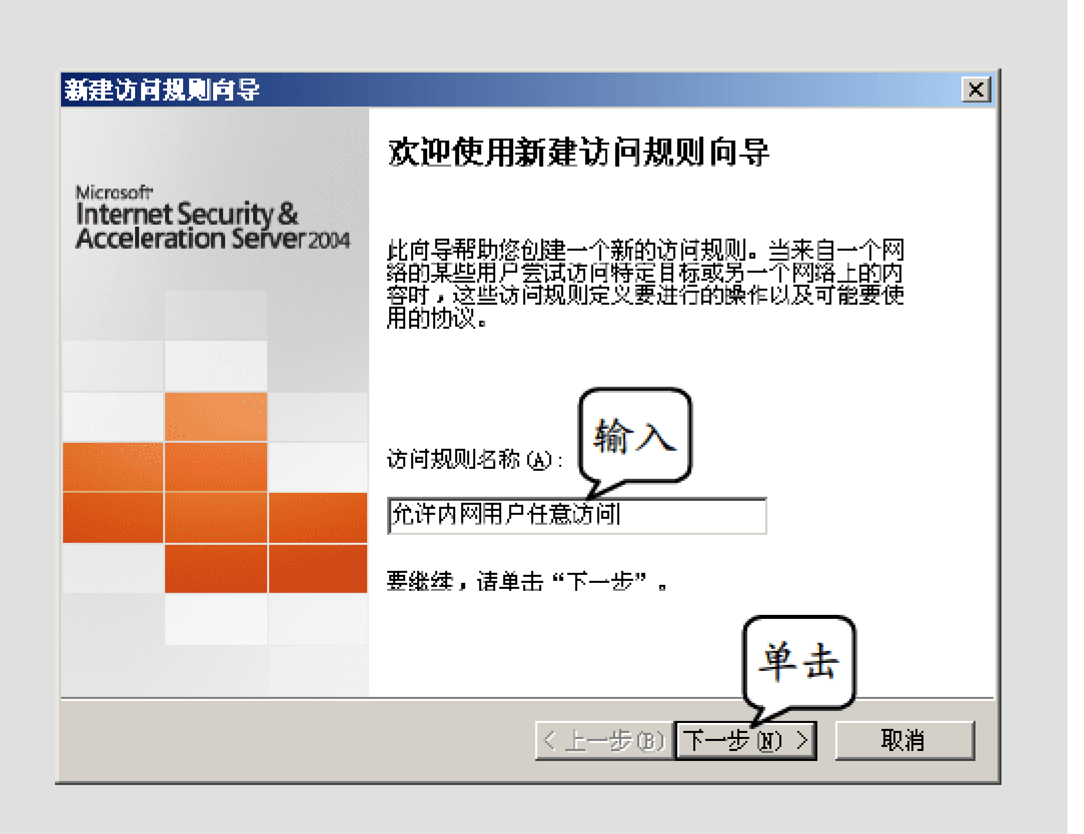


图 9-37　【欢迎使用新建访问规则向导】对话框

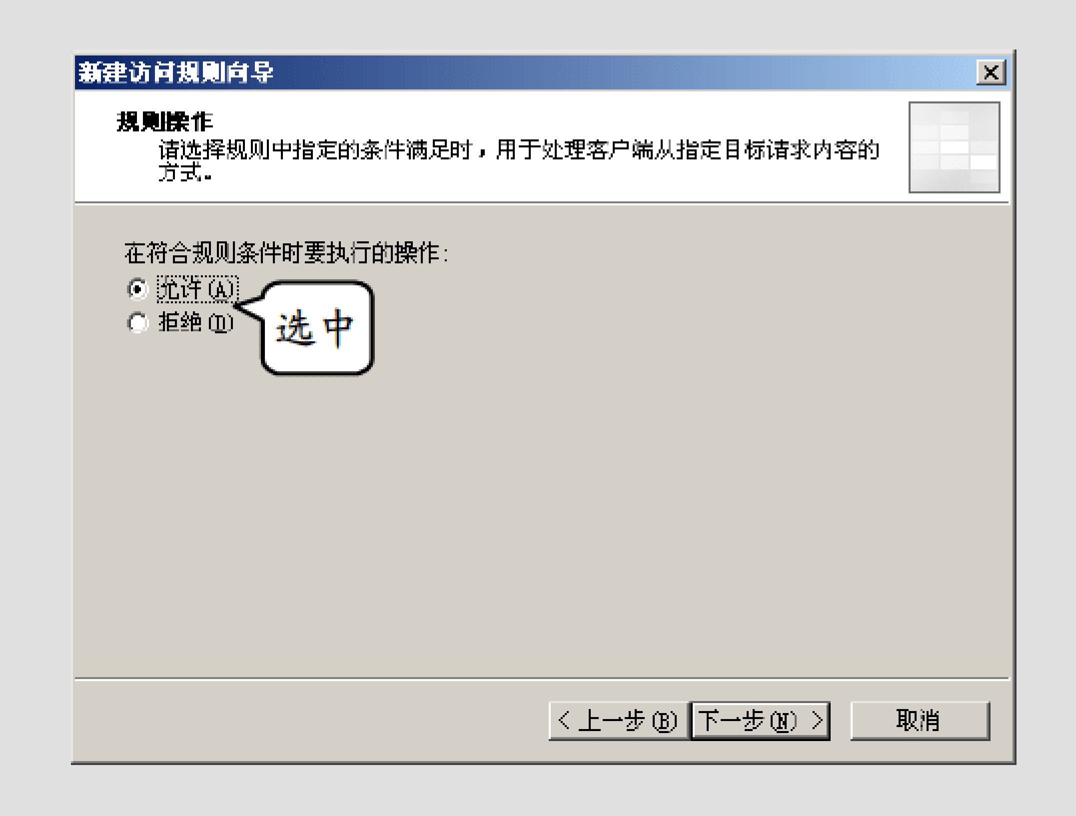


图 9-38　【规则操作】对话框

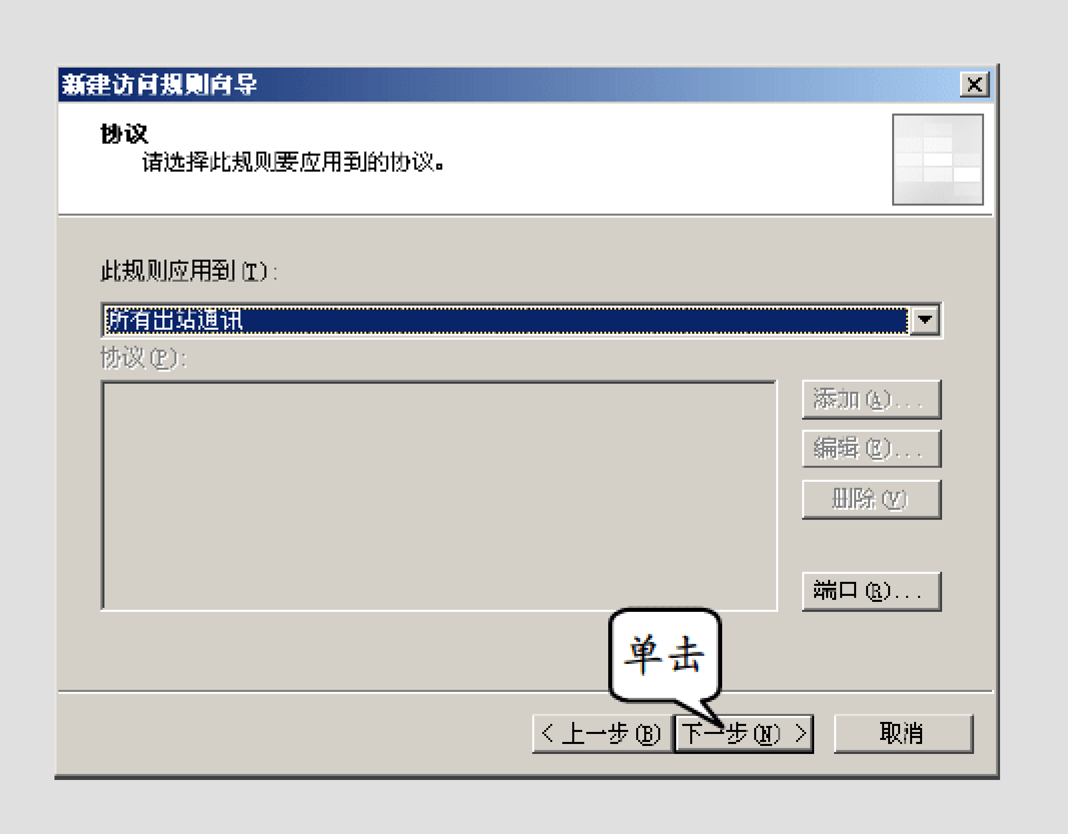


图 9-39　【协议】对话框

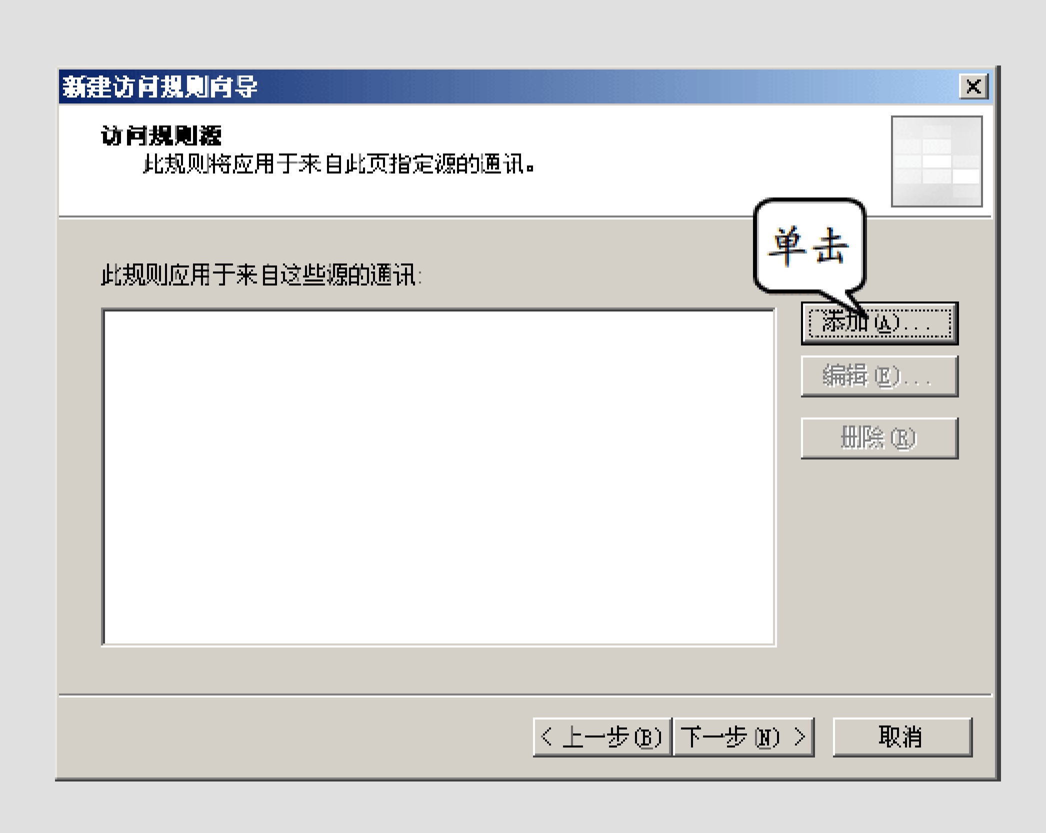


图 9-40　【访问规则源】对话框



图 9-41　【添加网络实体】对话框

（23）在【访问规则源】对话框中，单击【下一步】按钮，如图 9-42 所示。

（24）在【访问规则目标】对话框中，单击【添加】按钮，如图 9-43 所示。

（25）在弹出的【添加网络实体】对话框中，双击【网络】选项，选择【外部】选项，并依次单击【添加】和【关闭】按钮，如图 9-44 所示。

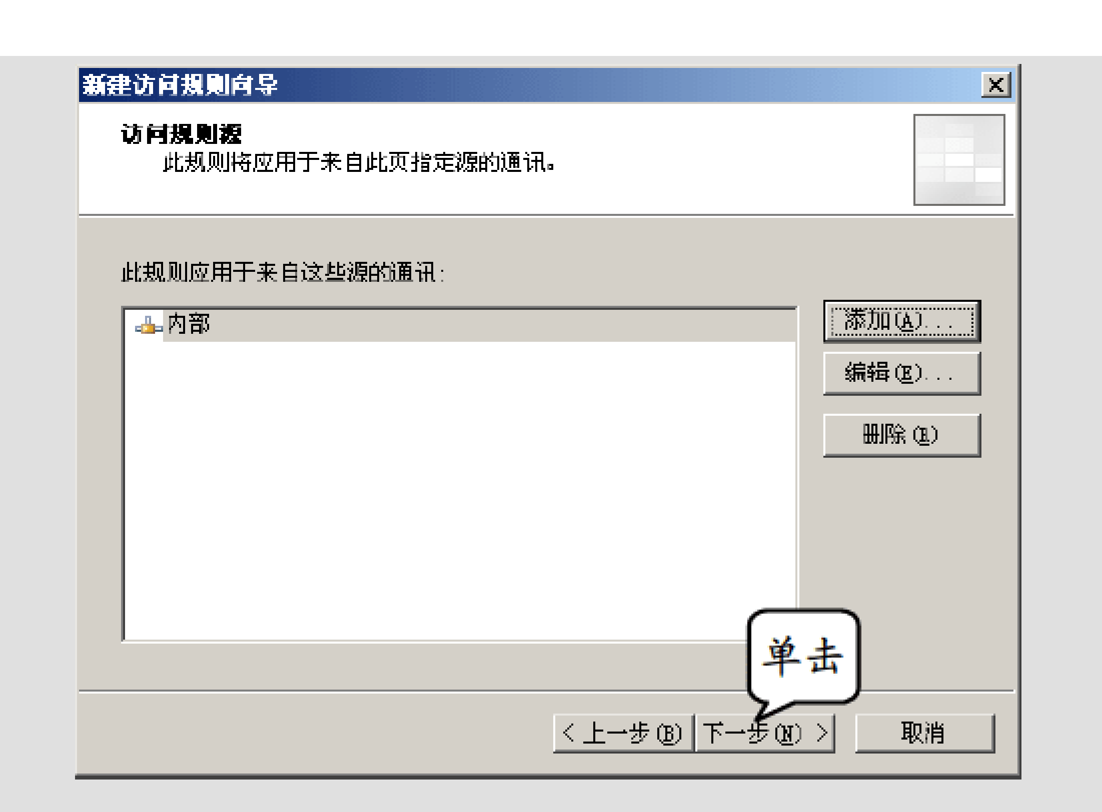


图 9-42 【访问规则源】对话框



图 9-43 【访问规则目标】对话框

（26）在【访问规则目标】对话框中，单击【下一步】按钮，如图 9-45 所示。





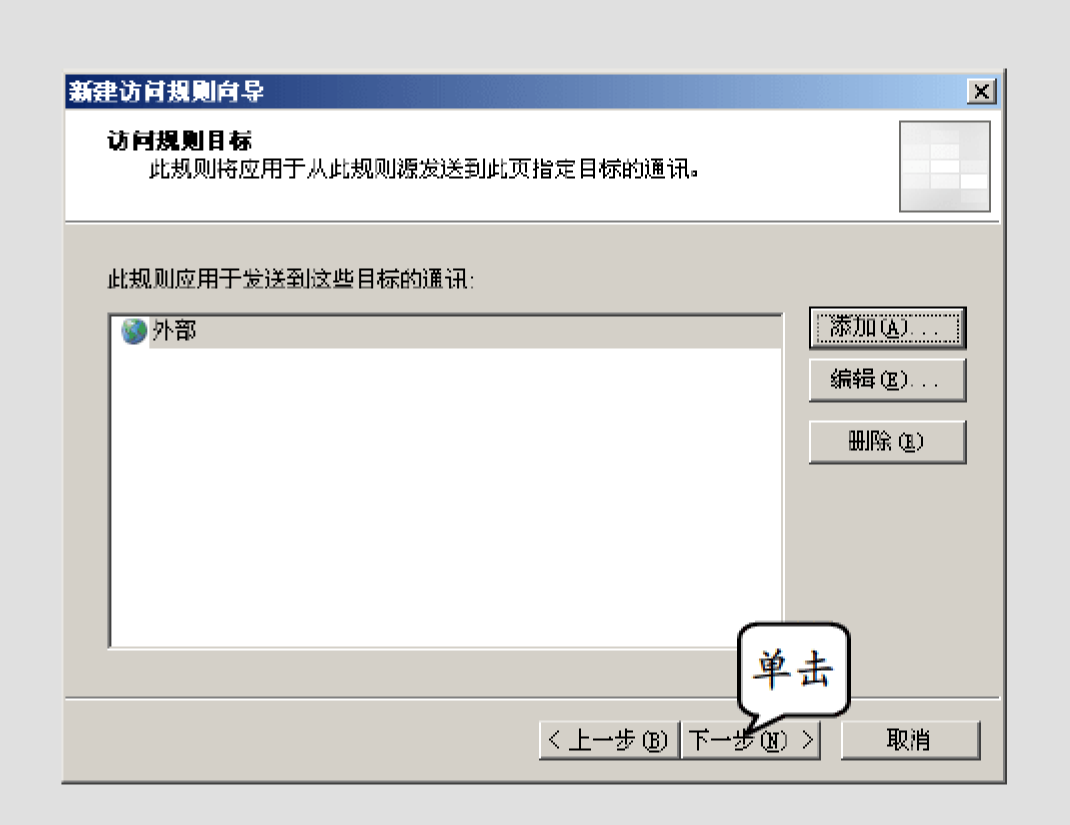
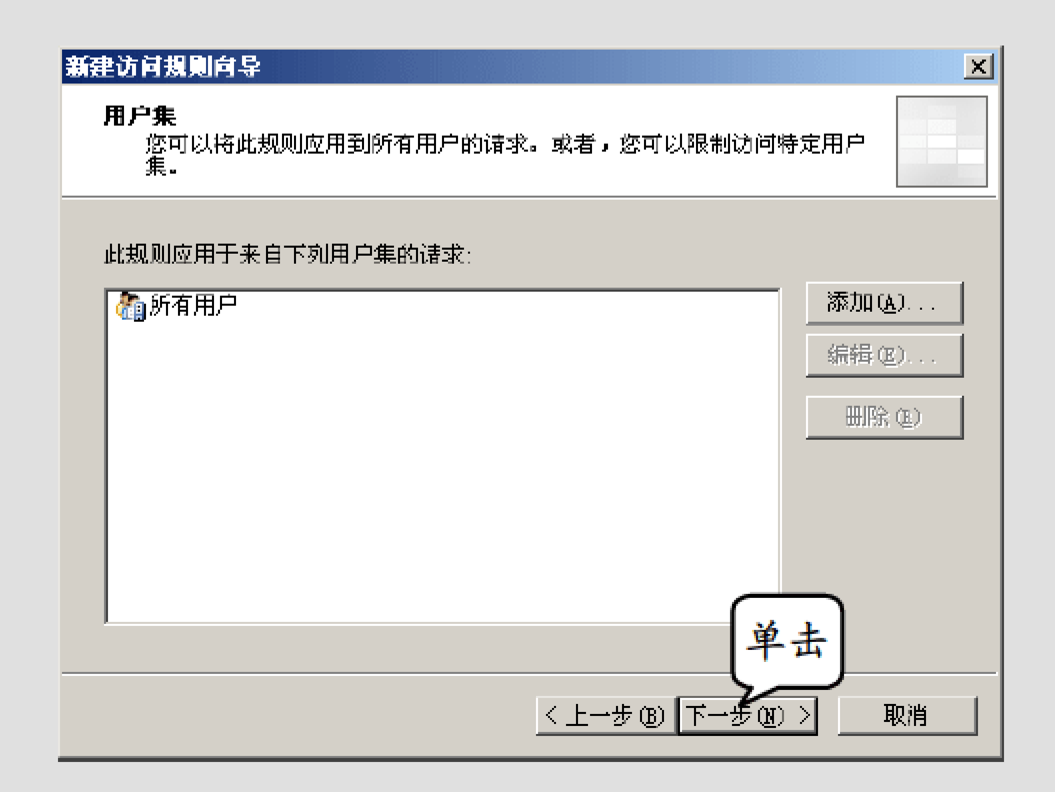


图 9-44 【添加网络实体】对话框

图 9-45 【访问规则目标】对话框

（27）在【用户集】对话框中，单击【下一步】按钮，如图 9-46 所示。

（28）在【正在完成新建 访问规则 向导】对话框中，单击【完成】按钮，如图 9-47 所示。



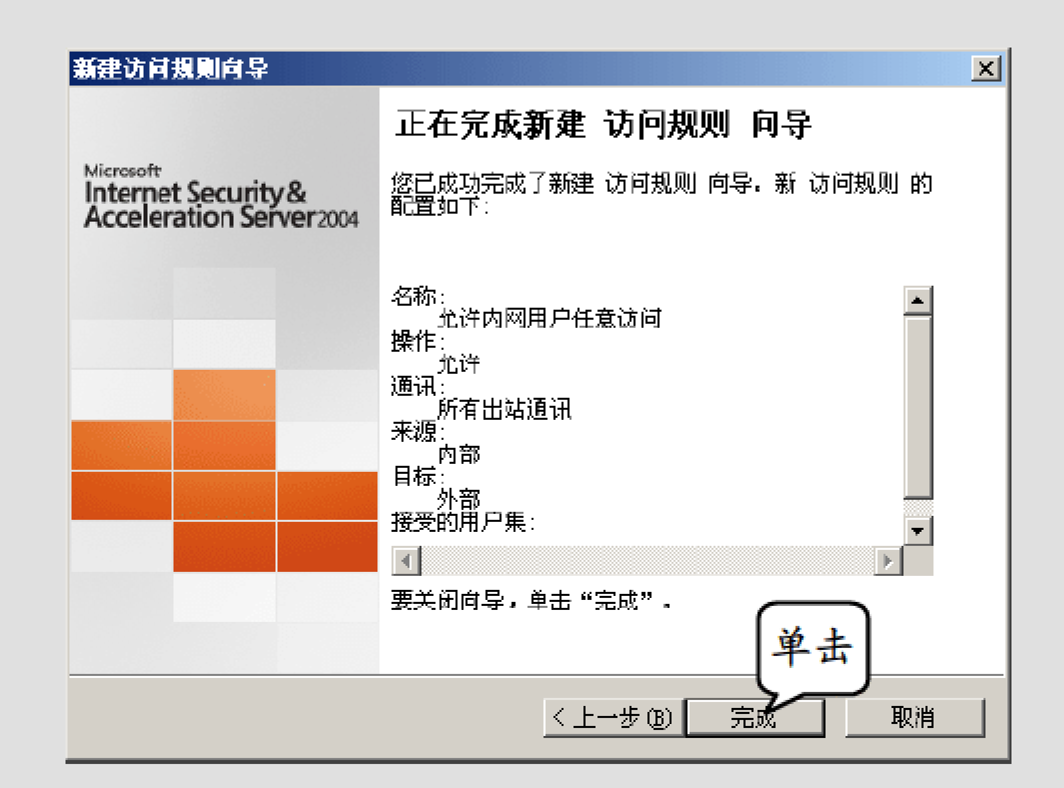


图 9-46 【用户集】对话框

图 9-47 新建访问规则向导完成

（29）在返回的 ISA Server 2004 Enterprise Edition 窗口中，单击【应用】按钮，如图 9-48 所示。

（30）在弹出的【正在保存配置更改】窗口中，单击【确定】按钮，如图 9-49 所示。

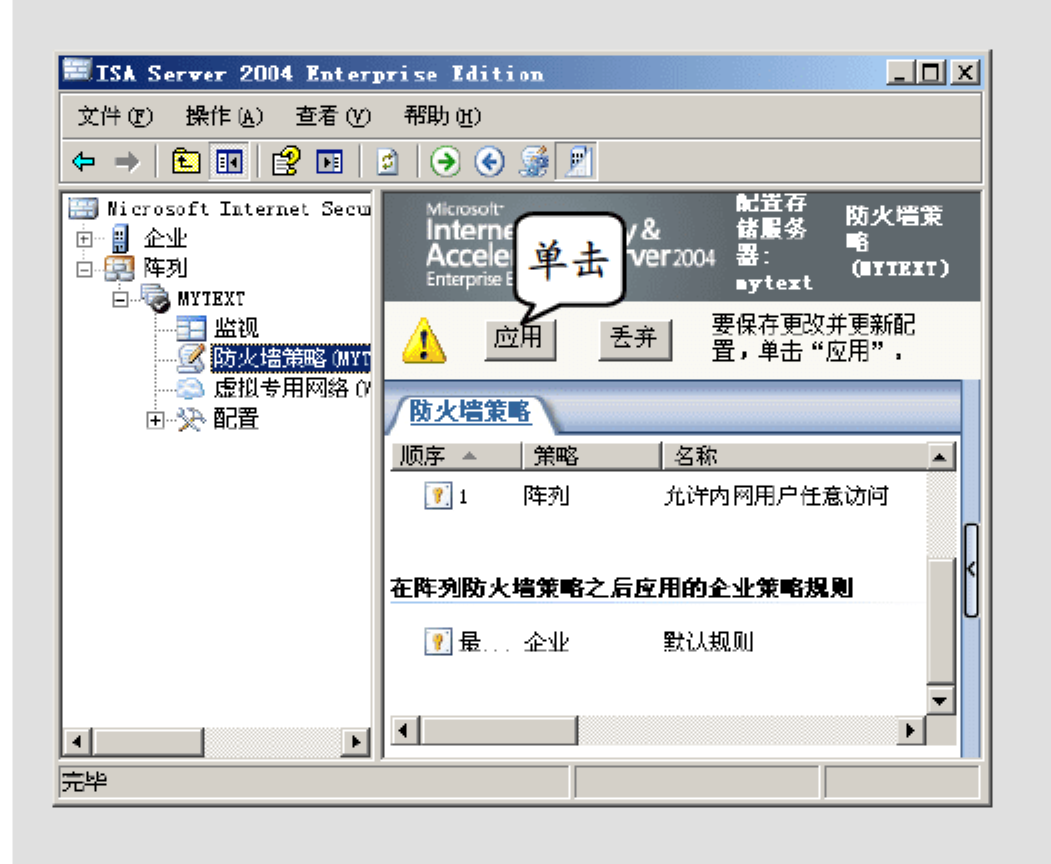


图 9-48　应用访问策略

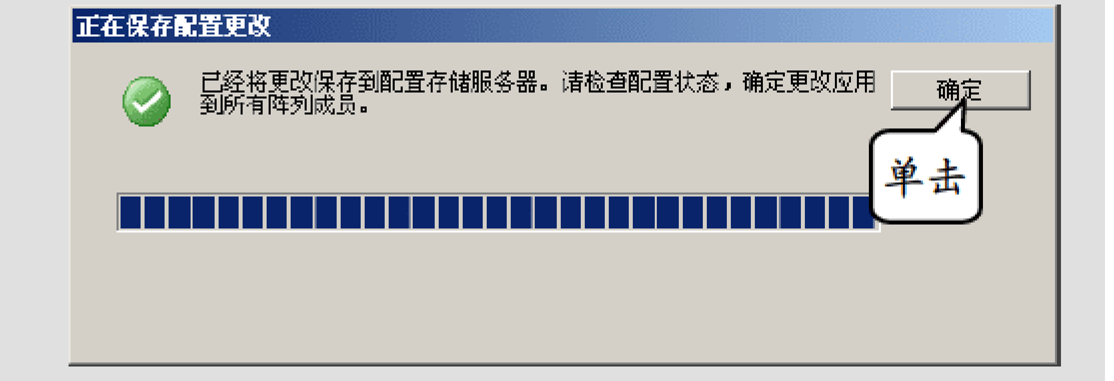


图 9-49　保存配置

（31）在内网客户端计算机上，双击 Internet Explorer 图标，单击菜单栏【工具】菜单，执行【Internet 选项】命令，如图 9-50 所示。

（32）在【Internet 选项】对话框中，选择【连接】选项卡，如图 9-51 所示。

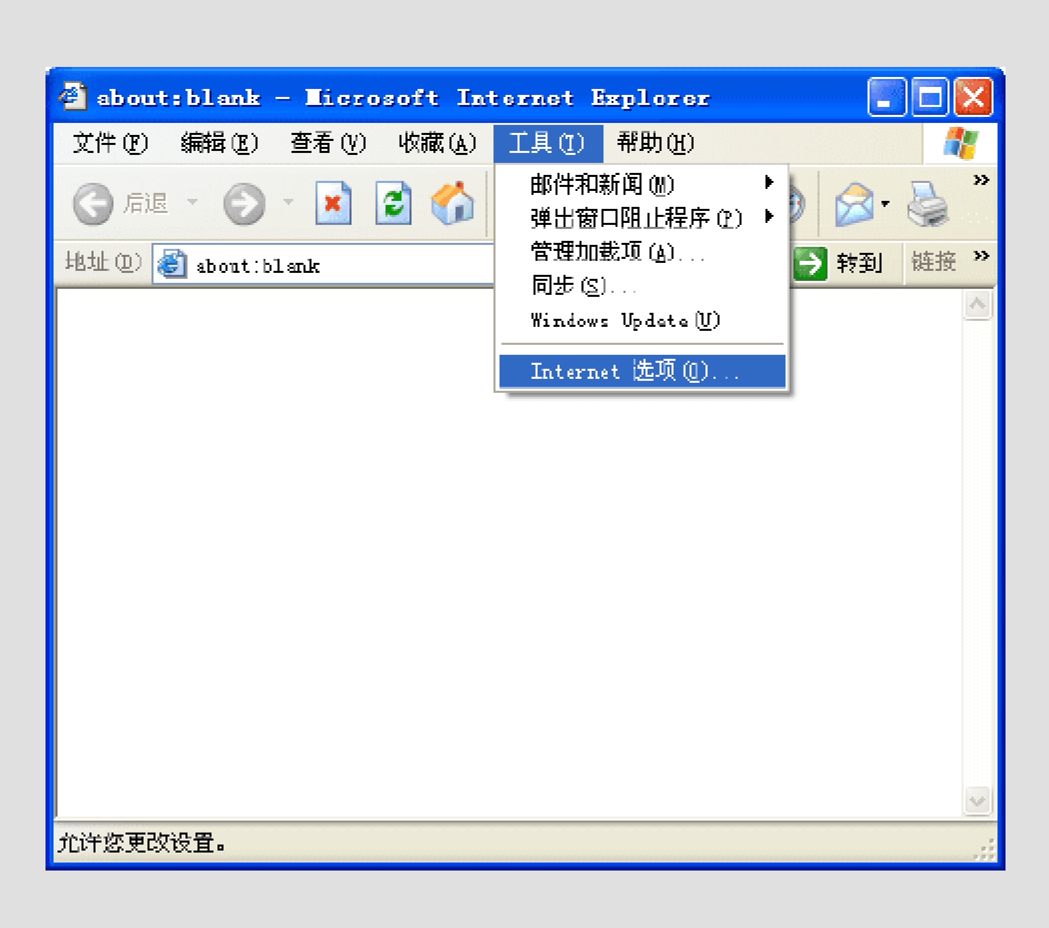


图 9-50　执行【Internet 选项】命令

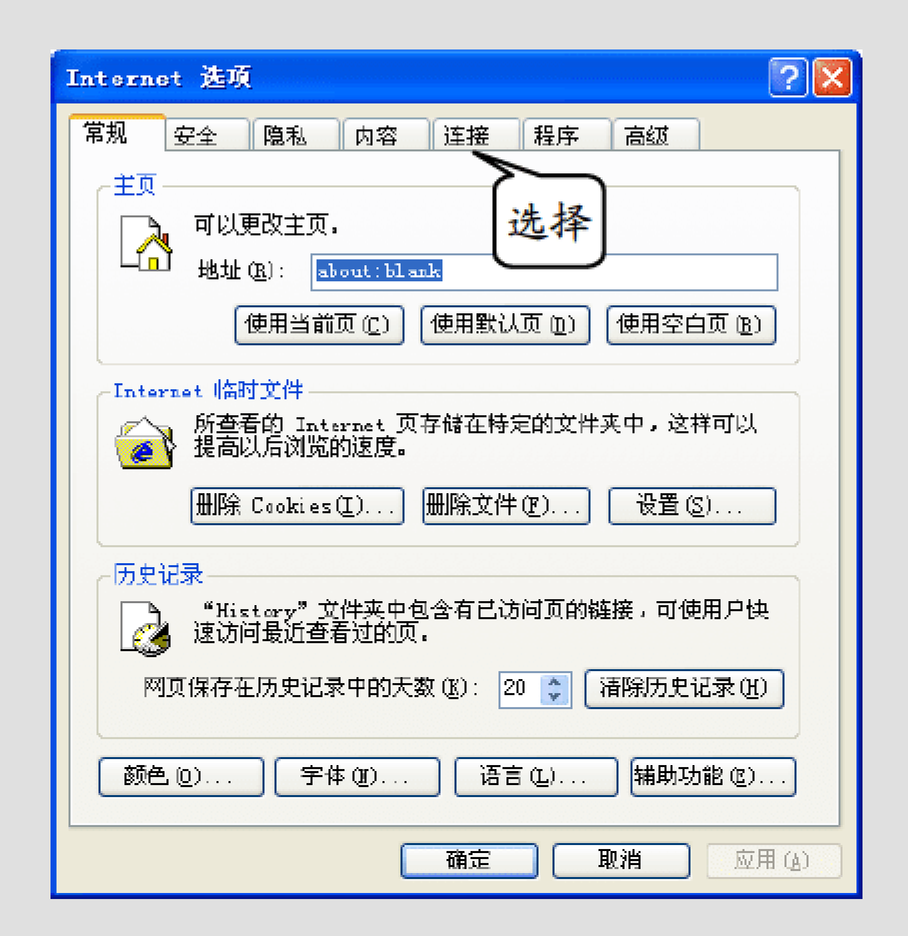


图 9-51　【Internet 选项】对话框

（33）在【连接】选项卡中，单击【局域网设置】按钮，如图 9-52 所示。

（34）在弹出的【局域网（LAN）设置】对话框中，启用【为 LAN 使用代理服务器】复选框，然后在【地址】和【端口】文本框中，分别输入“10.1.1.254”和“8080”，并单击【确定】按钮，如图 9-53 所示。



ISA 服务器的内网接口地址为 10.1.1.254，使用 8080 端口提供 Web 代理服务。

（35）在内网计算机桌面上，执行【开始】|【运行】命令，然后在【打开】文本框中，输入 www.baidu.com 命令，并单击【确定】按钮，如图 9-54 所示。

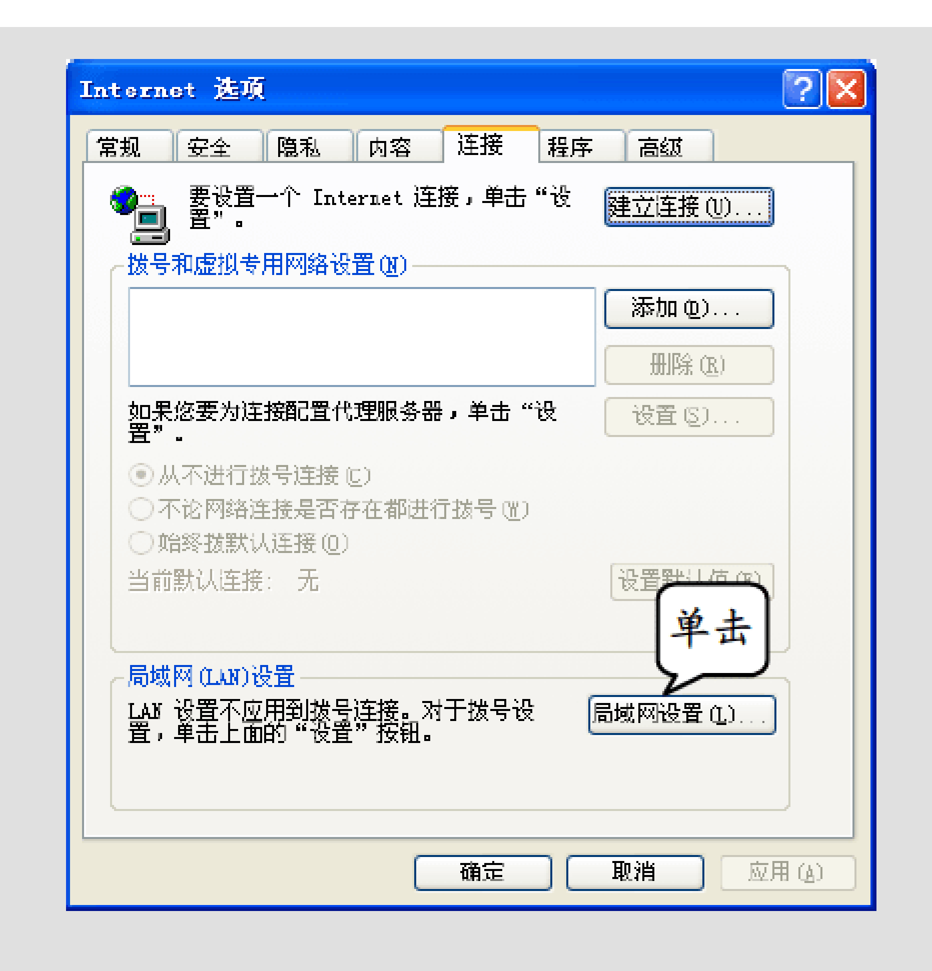


图 9-52 【连接】选项卡

图 9-53 【局域网（LAN）设置】对话框

（36）查看运行结果，如图 9-55 所示。



图 9-54 【运行】对话框



图 9-55 查看运行结果

9.5.2 操作实例——使用风云防火墙

风云防火墙为用户提供网络拦截、特征码防御、主动防御、ARP 防御、密码框保护五个功能，能够制定严密的访问规则，实时监控应用程序和系统进程，以及网络资源的访问。

1. 实例目的

- ❑ 制定 IP 端口过滤规则。
- ❑ 禁止访问共享资源。

2. 实例步骤

（1）在桌面执行【开始】|【程序】|【风云防火墙】|【风云防火墙个人版 2009】命令，如图 9-56 所示。

（2）在【风云防火墙个人版 2009 未注册】窗口中，选择【IP 端口过滤规则】选项卡，如图 9-57 所示。



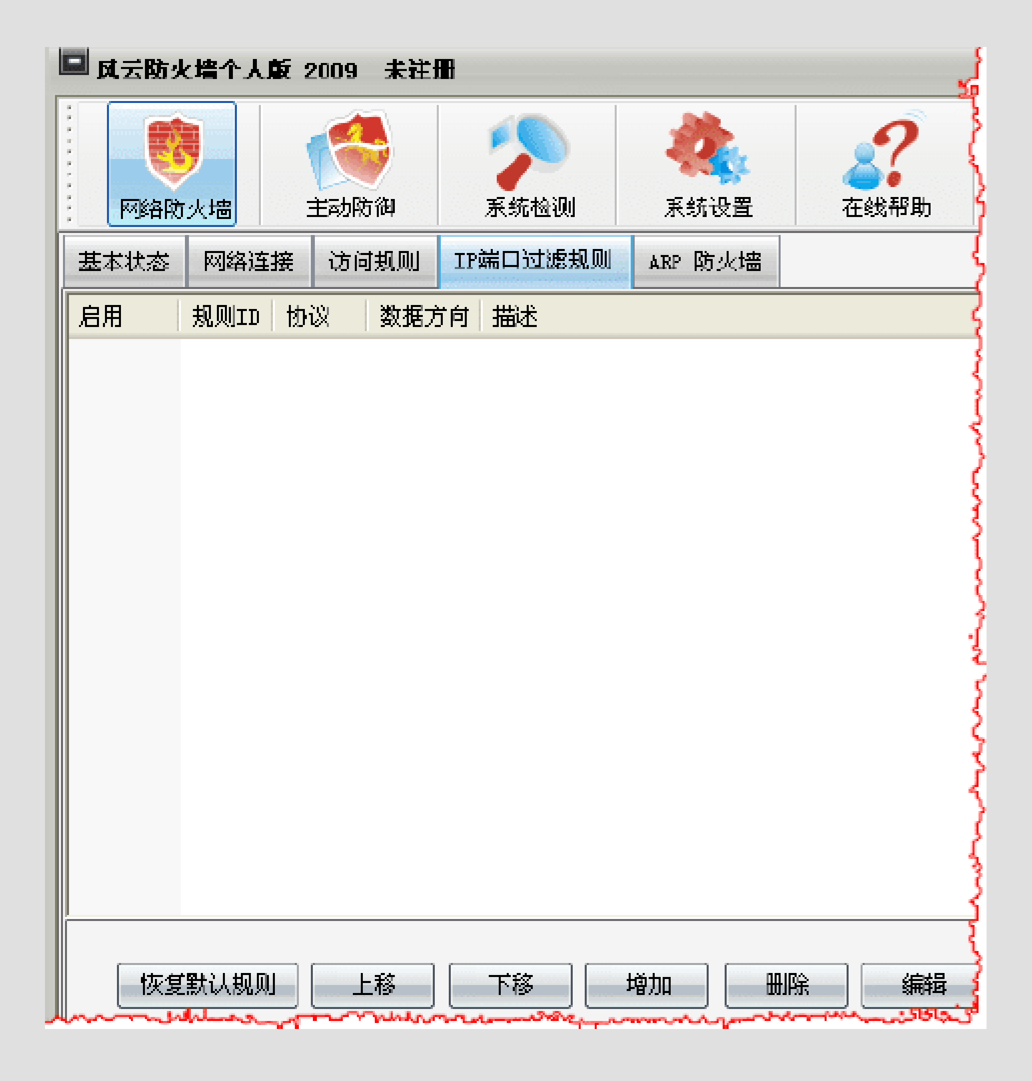
图 9-56　执行应用程序



图 9-57　风云防火墙主界面

（3）在【IP 端口过滤规则】选项卡中，单击【增加】按钮，如图 9-58 所示。

（4）在弹出的【增加规则】对话框中的【名称】文本框中，输入名称，如“禁止访问我的共享 1”，并在【本地端口（0-65535）】区域文本框中，分别输入“139”，然后单击【确定】按钮，如图 9-59 所示。



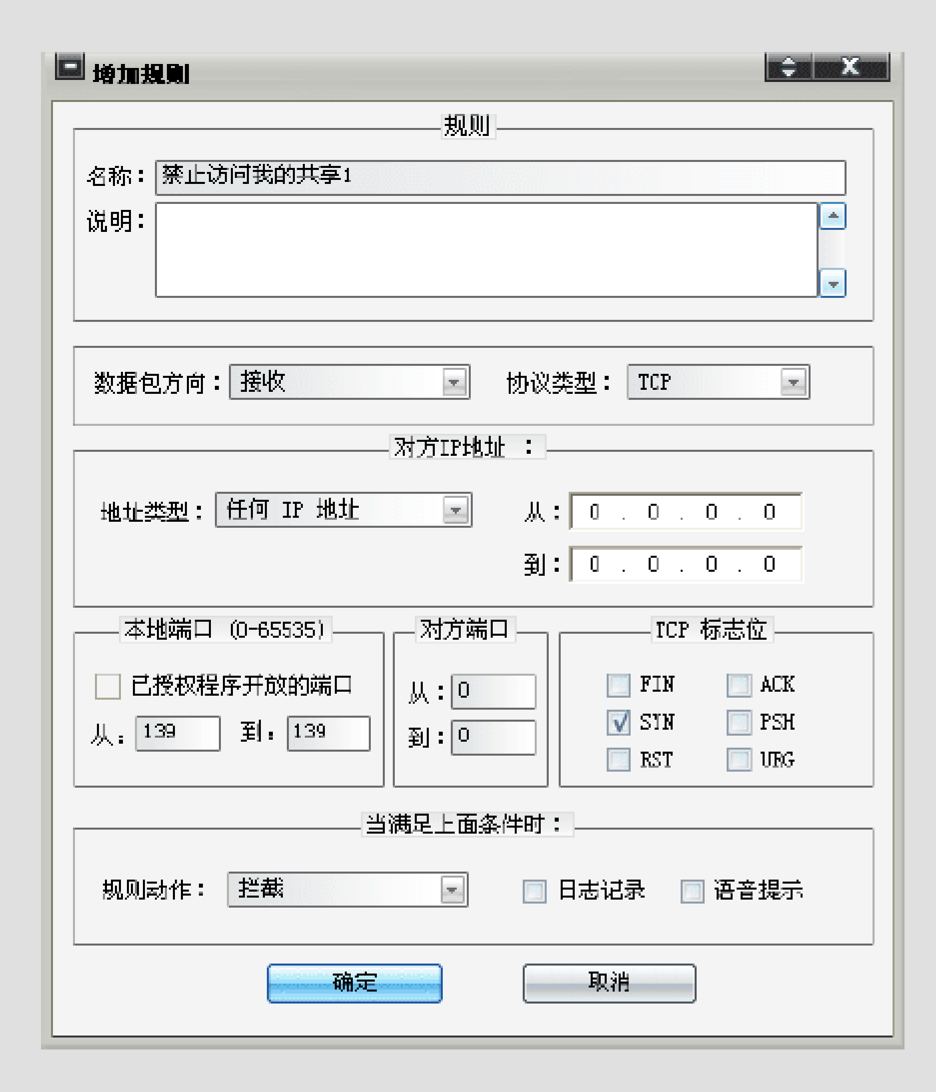


图 9-58　【IP 端口过滤规则】选项卡

图 9-59　【增加规则】对话框

（5）在【IP 端口过滤规则】选项卡中单击【增加】按钮，如图 9-60 所示。

（6）在弹出的【增加规则】对话框中的【名称】文本框中，输入名称，如“禁止访问我的共享 2”，并在【本地端口（0-65535）】区域文本框中，分别输入“445”，然后单击【确定】按钮，如图 9-61 所示。

（7）在客户端执行【开始】|【运行】命令，输入\\192.168.0.2\zw 命令，并单击【确定】按钮，如图 9-62 所示。

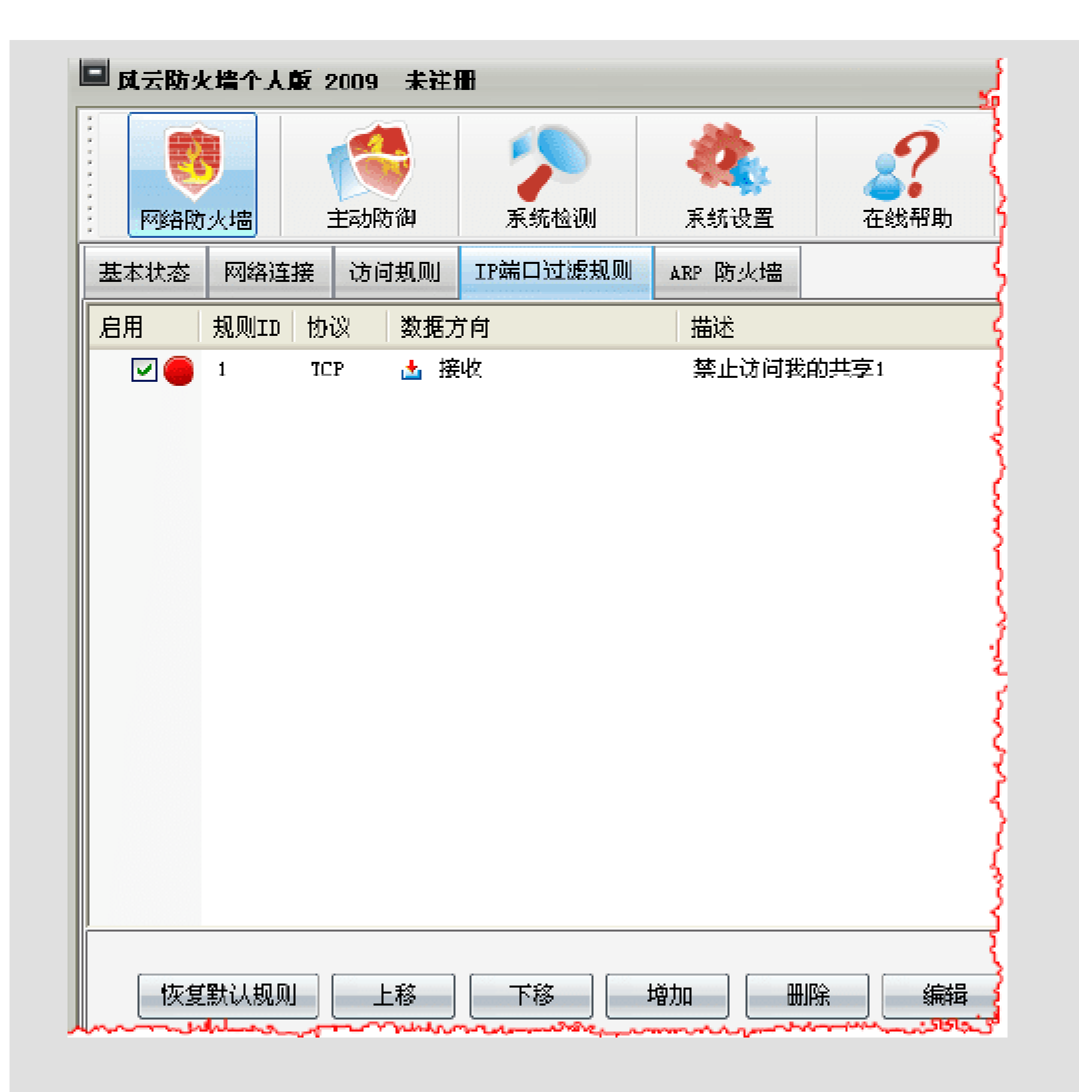


图 9-60 【IP 端口过滤规则】选项卡



图 9-61 【增加规则】对话框



服务器共享资源路径为\\192.168.0.2\zw。

（8）查看访问结果，如图 9-63 所示。

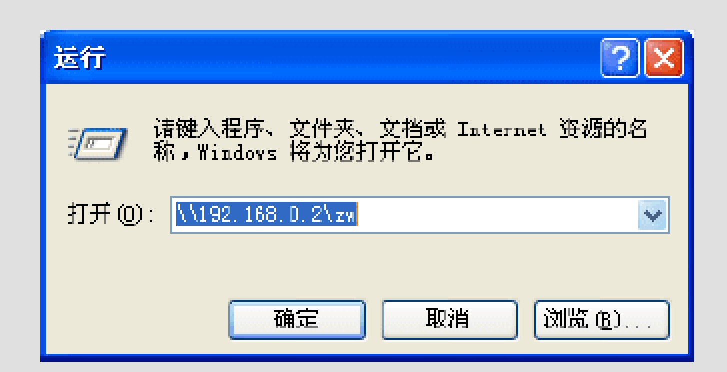


图 9-62 【运行】对话框

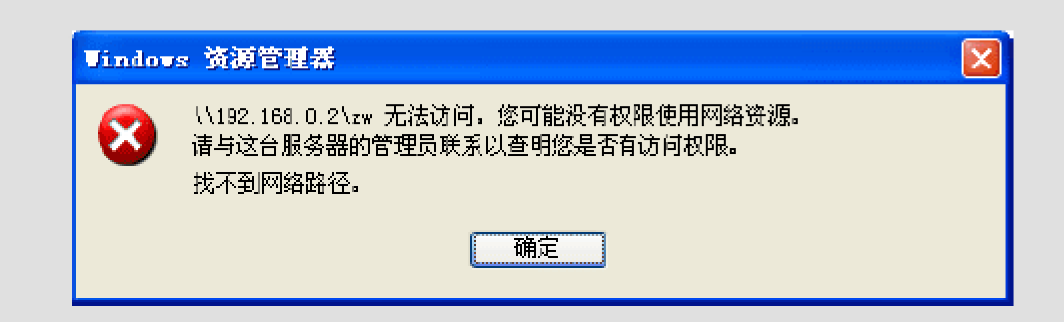


图 9-63 【Windows 资源管理器】对话框



Windows XP 系统提供共享服务的端口为 139 端口，Windows 2003 系统提供共享服务的端口为 445 端口。

第10章 Cisco PIX 防火墙

随着 Internet 的进一步普及和迅猛发展，针对内网计算机的入侵事件日益增多，应用防火墙技术势在必行。但防火墙产品种类繁多，功能上也存在很大差异，这给防火墙系统的实现和维护带来了许多难题。通常一个完整的防火墙系统既要防止外部入侵，又要防止内部人员的非法访问。而对于 Cisco PIX 防火墙来说，利用动态和静态地址翻译、管道等技术，可以很方便地实现这一完整的防火墙系统。

本章学习要点：

- PIX 防火墙概述
- PIX 防火墙的基本使用
- PIX 防火墙的高级配置

10.1 PIX 防火墙的概述

目前，防火墙包括集成防火墙功能的路由器、集成防火墙功能的代理服务器、专用软件防火墙和专用的软硬件结合的防火墙 4 种类型，而在 Cisco 的防火墙解决方案中包含了 4 种类型的第 1 种和第 4 种，即集成防火墙功能的路由器和专用的软硬件结合的防火墙。

Cisco PIX（Private Internet Exchange）防火墙，属于 4 类防火墙中的第 4 种，它的设计是为了满足高级别的安全需求，以较好的性能价格比提供严密的、较有力的安全防范。

10.1.1 PIX 防火墙的功能特点

一般来说，防火墙系统就是在两个网络之间实施的一些存取控制方法的集合。通常有两种类型的防火墙，基于网络层的包过滤防火墙和基于应用层的隔离网络的代理服务器（Proxy Server）。

基于网络层的包过滤防火墙，主要是在网络层根据 IP 数据包的源和目标地址，及源和目标端口来决定是转发还是丢弃 IP 数据包；而基于应用层的隔离网络的代理服务器，则是在应用层为每一种服务提供一个代理。

Cisco PIX 防火墙是基于这两种技术结合的防火墙，它应用安全算法（Adaptive Security Algorithm，ASA），将内部计算机的地址映射为外部地址，拒绝未经允许的数据包进入，实现了动态、静态地址映射，从而有效地屏蔽了内部网络拓扑结构。通过管道技术（conduit），访问列表（ACL）等可以有效地控制内、外部各资源的访问。

另外，PIX 防火墙可连接 4 个不同的网络，每个网络都可定义一个安全级别，级别低的相对于级别高的总是被视为外部网络，从而安全地保证了内部网络。

10.1.2 PIX 防火墙的算法与策略

PIX 防火墙中的安全算法，是一种基于状态的安全防护方式。每个进来的数据包（从位于较低安全级别网络的计算机到位于较高安全级别网络的计算机）都要根据它和 PIX 防火墙内存中的连接状态信息进行检查。ASA 信息是实施 Internet 访问安全的基础，因为它可执行如下任务。

- ❑ 经过 PIX 防火墙执行状态连接控制。
- ❑ 针对每个内部系统应用，在没有明确配置的情况下，允许单向（出站）连接。出站的连接从位于较高安全级别接口的计算机访问位于较低级别网络的计算机。
- ❑ 监控返回的数据包，确认它们的有效性。
- ❑ 对 TCP 顺序号进行随机处理，减少被攻击的可能性。

ASA 在 PIX 防火墙控制的网络之间构成安全边界。ASA 在设计上是基于状态的面向连接的，能够创建基于源和目标地址的会话流；在完成连接之前，能够对 TCP 顺序号、端口号和 TCP 标记进行随机处理。这个功能始终都在运行，监视每个返回的数据包，确认它们的正确性。

在 ASA 中，安全级别用来表明一个接口相对于另一个接口是可信（较高的安全级别）还是不可信（较低安全级别）的。

如果一个接口的安全级别高于另一个接口的安全级别，这个接口就被认为是可信的；如果一个接口安全级别低于另一个接口的安全级别，这个接口就被认为是不可信的，如图 10-1 所示。

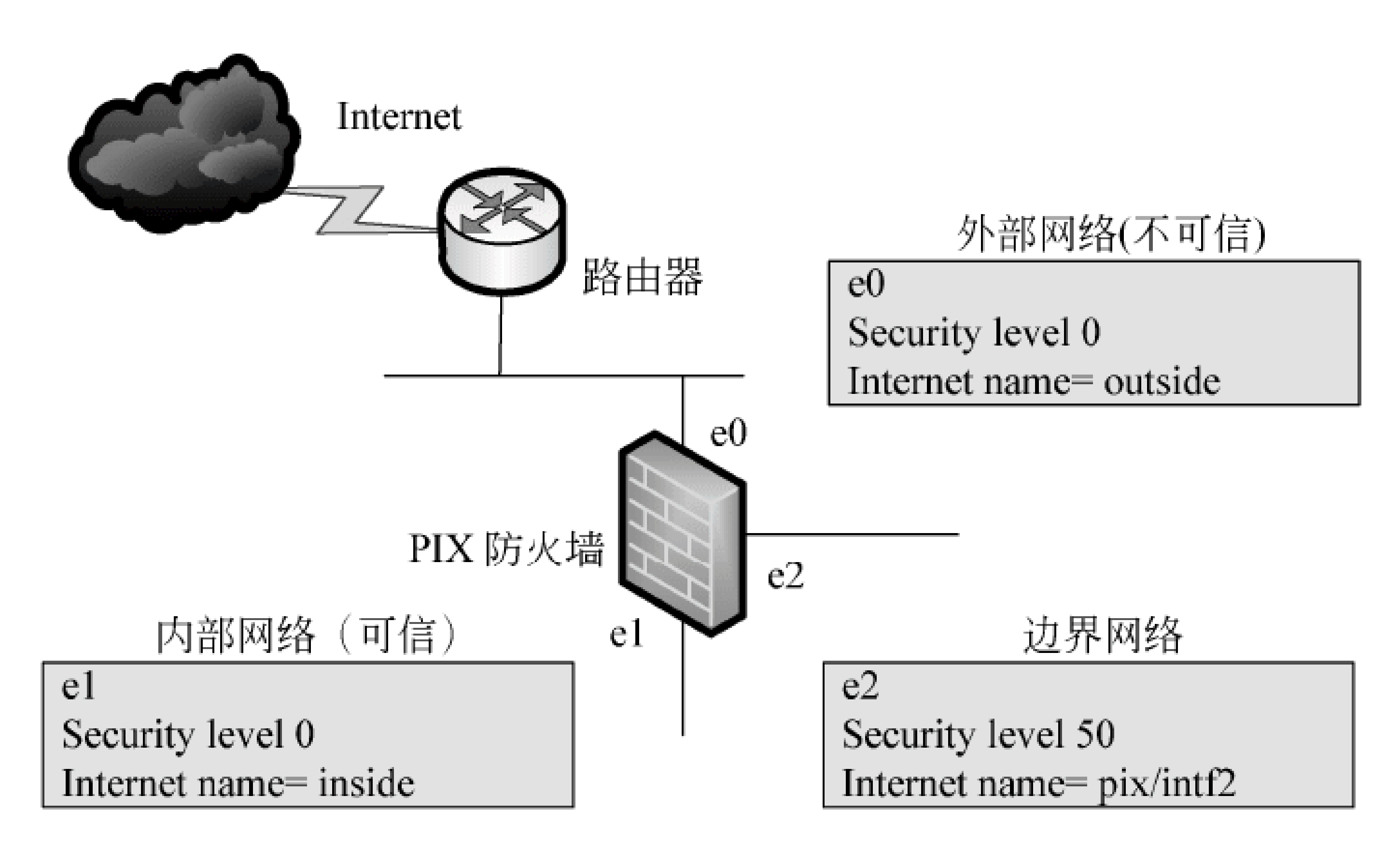


图 10-1　PIX 防火墙接口安全级别

安全级别的基本策略是具有较高安全级别的接口可以访问具有较低安全级别的接口。反过来，在没有设置管道（conduit）和访问控制列表（ACL）的情况下，具有较低安全级别的接口不能访问具有较高安全级别的接口，安全级别的范围从 0～100。下面是有关这些安全级

别的更具体规则。

❑ **安全级别 100**

这是 PIX 防火墙内部接口的最高安全级别，也是 PIX 防火墙的默认设置，且不能改变。安全级别 100 是最值得信任的接口安全级别，所以应该将公司网络建立在这个接口的后面。这样，除非经过特定的允许，否则其他的接口都不能访问这个接口，但这个接口后面的每台设备都可以访问公司网络外面的接口。

❑ **安全级别 0**

这是用在 PIX 防火墙外部接口的最低安全级别，防火墙的默认设置，且不能更改。因为 0 是不值得信赖的最低级别，所以应该把最不值得信任的网络连接到这个接口的后面。这样，除非经过特定的许可，否则它不能访问其他接口。这个接口通常用于连接 Internet。

❑ **安全级别 1～99**

这些是分配与 PIX 防火墙相连的边界接口的安全级别。可以根据每台设备的访问情况来给它们分配相应的安全级别。

10.1.3 网管心得——PIX 防火墙系列产品介绍

从 1996 年以来，为了更好地满足小型和大型客户网络安全的需求，Cisco 将 PIX 防火墙系列产品扩展到 PIX501、PIX506E、PIX515E、PIX525 和 PIX535 5 种不同的型号，能够满足广泛的用户需求和不同大小的网络规模。目前，这些 PIX500 系列防火墙产品适用的市场如图 10-2 所示。



图 10-2 PIX500 系列防火墙产品

❑ **PIX501 防火墙**

PIX501 防火墙是 5 种型号中最小的一种，是为远距离办公者或小型办公室/家庭办公而设计的。它集成了一个 4 端口的交换机，并对外提供一个 10/100Mbps 的快速以太网接口，如图 10-3 所示。

❑ **PIX506E 防火墙**

PIX506E 防火墙是为小型办公室和远程办公设计的，它集成了两个 10/100Mbps 以太网接

口，如图 10-4 所示。

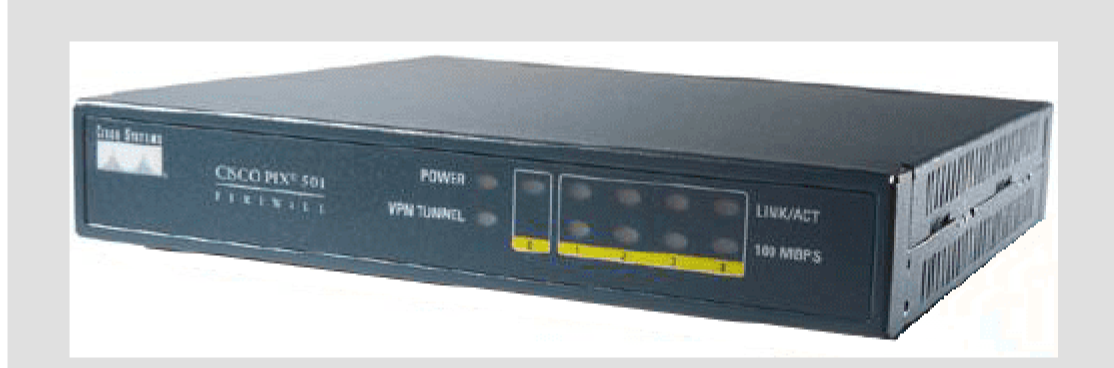


图 10-3 PIX501 防火墙



图 10-4 PIX506E 防火墙

❑ **PIX515E 防火墙**

PIX515E 防火墙是为小型到中型商业设计的，它支持 6 个 10/100Mbps 以太网接口，如图 10-5 所示。

❑ **PIX525 防火墙**

它是为大型商业和企业用户设计的，它支持 8 个 10/100Mbps 快速以太网和吉比特以太网接口，如图 10-6 所示。

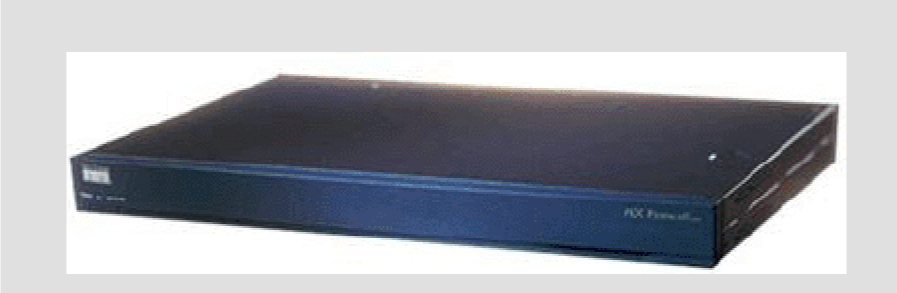


图 10-5 PIX515E 防火墙

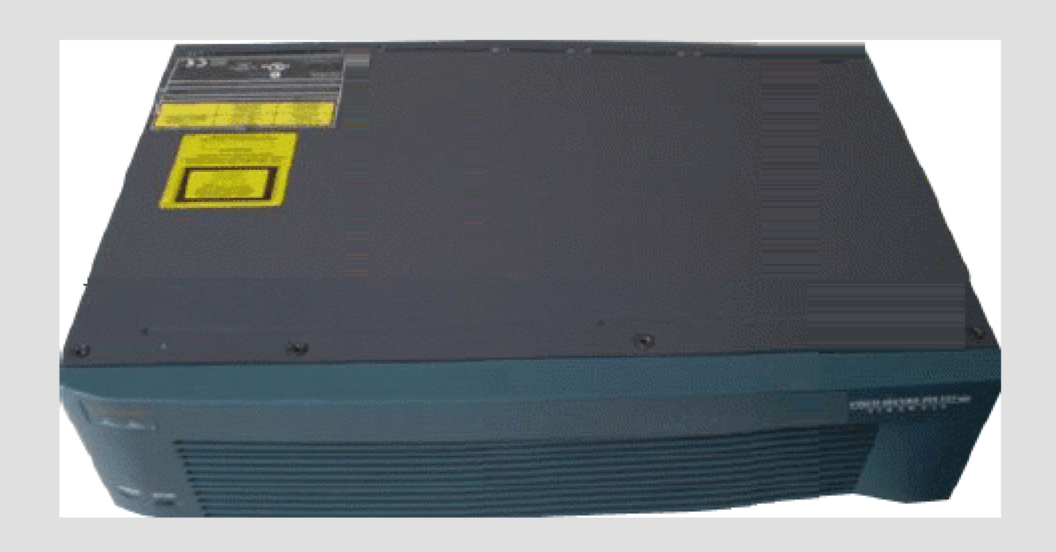


图 10-6 PIX525 防火墙

❑ **PIX535 防火墙**

在 500 系列中最强大的产品，PIX 防火墙 535 是为企业级和服务提供商用户设计的，它支持多达 10 个 10/100Mbps 快速以太网和吉比特以太网接口，如图 10-7 所示。



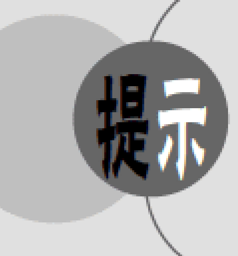
图 10-7 PIX535 防火墙

在这些 PIX500 防火墙系列产品中，每一款都具有强大的保护功能。如 PIX515E 防火墙是针对于小型和中型企业设计的，它具有完整的防火墙保护能力，并且通过 IPSec 相应的加密标准（56bit DES、168 bit DES）搭建 VPN 的能力。在两个 PIX 防火墙之间可以搭建 VPN 隧道，PIX 防火墙同样可以与以下设备之间搭建 VPN 隧道。

❑ 任何支持 VPN 的 Cisco 路由器。
❑ Cisco 3000 VPN 集中器。
❑ 支持 IPSec 标准的设备。

PIX515E 防火墙同样适用于只与总部网络之间建立双向通信的远程计算机。另外，它还支持基于精简的 IPSec 加速，能够提供 140Mbps 的吞吐量，同时把系统资源让给其他更加重要的安全功能。

PIX515E 防火墙设计为机架式，拥有 433MHz 的处理器，32MB 或 64MB 的 CDROM（只读存储器）和 16MB 的内存。



通过使用可选的 PIX 防火墙 VAC 或者高性能的 VAC+来提供 IPSec 加速，当没有安装 VAC 和 VAC+时，PIX 防火墙 515E 运行在基于加密环境下，则导致吞吐量下降。

10.2　PIX 防火墙的基本使用

PIX 防火墙的基本使用是实现其功能的基础，因此可通过防火墙自身具有命令行（CLI）方式，进行如系统显示名称、端口 IP 地址及定义路由等简单配置。

10.2.1　PIX 防火墙的基本命令

PIX 防火墙支持基于 Cisco IOS（Internetwork Operating System，互联网络操作系统）的命令集，并提供了多种管理访问模式。

1. PIX 防火墙的模式

每台 Cisco PIX 防火墙设备均支持不同的访问模式，对于与 CLI（Command Line Interface，命令行界面）的交换，大体可以分为 4 种常见的模式。

- **非特权模式**　PIX 防火墙开机自检后，处于这种模式。系统显示为“pixfirewall>”。
- **特权模式**　在非特权模式下，输入 enable 进入该模式，可更改当前配置。系统显示为“pixfirewall#”。
- **全局配置模式**　在特权模式下，输入 configure terminal 进入此模式，绝大部分的系统配置都在这里进行。系统显示为“pixfirewall(config)#”。
- **监控模式**　PIX 防火墙在开机或重启过程中，按 Escape 键，进入监控模式。在此，可以更新系统映像和口令恢复。系统显示为“monitor>”。

在每种访问模式下，可把大多数命令缩写成最少且唯一的字符串。例如，可以输入 write t 来查看配置信息，而不用输入完整的命令 write terminal。输入 en 代替 enable，进入特权模式；输入 config t 代替 configure terminal，进入全局配置模式。

在 PIX 防火墙命令行（CLI）中，可以获得帮助信息，输入 help 或？能够列出所有命令，如果一个命令后面输入？（如 route ?），会列出这个命令的语法。如果在一个命令的前面输入 help（如 help nameif），会列出这个命令的说明和语法。访问模式不同，使用问号或 help 命令时，列出的命令数量不同。在非特权模式下，列出的命令最少，在全局配置模式下，列出的命令最多。另外，在命令行中可以只输入命令本身，然后按回车键，也可以查看这个命令的语法。

和 Cisco IOS 路由器相比，PIX 防火墙 CLI 环境的一个突出优点是，在全局配置模式下可执行所有的命令，而不必从全局配置模式退出来，即可直接使用所有 show 和 debug 命令，列出正在运行的和当前保存的配置。

2. 基本配置命令

在学习 PIX 防火墙时，应该了解一些基本的命令，如查看、保存、清除配置及命名和重启防火墙等。

❑ **enable 命令**

输入 enable 命令后，PIX 防火墙将提示输入特权模式密码，默认没有密码，所以在提示输入密码时，可直接按回车键，当然也可以创建一个密码。可在全局配置模式下，使用 enable password 命名设置该密码。密码对大小写敏感，长度 3 到 16 个数字或字母，除了问号、空格、冒号外，可以使用任何字符。

命令的语法如下所示。

```
Pixfirewall(config)#enable passwork password [level priv_level] [encrypted]
```

- **priv_level** 表明特权模式级别，从 0~15。
- **password** 设置的特权模式密码。
- **encrypted** 指明设置的密码将被加密。

❑ **查看、保存、清除配置命令**

命令 show running-config（在特权模式下）把 PIX 防火墙 PDM 中当前的配置显示在终端上，也可以使用命令 write terminal 来显示当前配置。

命令 write memory（在特权模式下）把当前正在运行的配置保存到闪存中，当配置写到闪存中后，可以通过命令 show startup-config 或 show running-config 来查看。

命令 write erase（在特权模式下）可以清除闪存中的配置，如果输入这个命令，提示确认是否想删除配置，此时按回车键即可清除。

```
Pixfirewall(config)#write erase
Erase PIX configuration in Flash memory? [confirm]
```

❑ **命名 PIX 防火墙**

命令 hostname（在特权模式下），可更改 PIX 防火墙系统显示名称，如果将其名称改为 firewall 时，则系统名称显示为 firewall#（特权模式）。

❑ **重启 PIX 防火墙命令**

命令 reload 可以让 PIX 防火墙重新启动，并从闪存中重新加载配置信息。在执行重新启动之前，系统会显示信息“process with reload?”提示确认。如果回答 Y 之外的任何其他信息，都会取消重新加载（reload）命令。

重新加载后，之前修改的配置，若没有保存到闪存中，都会丢失。在进行重新启动之前，应使用命令 write memory 把当前的配置保存到闪存中。

10.2.2 基本的 PIX 防火墙配置

在 PIX 防火墙上，可以使用 CLI（命令行界面）对其进行基本的配置。下面是对 PIX 防火墙进行配置时使用的一些基本配置命令。

❑ **nameif** 给每个边界接口分配一个名字，并指定安全级别。

- **interface**　配置每个边界接口的类型和能力。
- **ip address**　给每个接口分配 IP 地址。
- **nat**　对外部网络隐藏内网的 IP 地址。
- **global**　使用一个 IP 地址池对外部网络隐藏内网的 IP 地址。
- **route**　为一个接口定义一个静态或默认路由。

1. nameif

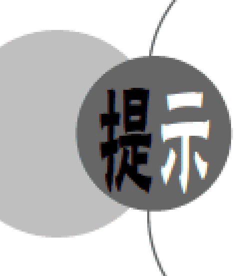
通过该命令，可以为 PIX 防火墙的每个边界物理或逻辑端口分配一个名字，并指定它们的安全级别（除 PIX 防火墙的内部和外部接口，它们的名字是默认的）。该命令的语法格式如下所示。

```
nameif hardware_id if_name security_level
clear nameif
show nameif
```

- **hardware_id**　指定边界接口和它在 PIX 中的插槽位置。每个接口名称由两部分组成，一部分是基于接口类型的字母，另一部分是给它分配的序号。例如，以太网接口可以用 e1、e2、e3 等来表示。
- **if_name**　对边界接口进行描述，所指定的名字在后面配置边界接口时可以引用。
- **security_level**　指明边界接口的安全级别，有效范围在 1~99 之间。

例如，配置防火墙接口的名称，并指定安全级别。

```
Pixfirewall(config)#nameif ethernet0 outside security 0
Pixfirewall(config)#nameif ethernet1 inside security 100
Pixfirewall(config)#nameif dmz security 50
```



在默认配置中，以太网 0 被命名为外部接口（outside），安全级别为 0；以太网 1 被命名为内部接口（inside），安全级别为 100。安全级别取值范围 0~100，数字越大安全级别越高。若添加新的接口，命令语法可以这样写：Pixfirewall(config)#nameif intf3 security 40（安全级别取任意值）。

2. interface

命令 interface 用来指明硬件、设置设备硬件的速度、启动接口，其命令语法格式如下所示。

```
interface hardware_id [hardware_speed] [shutdown]
clear interface
```

- **hardware_id**　指定边界接口和它在 PIX 中的插槽位置。
- **hardware_speed**　设置接口的连接速率。
- **shutdown**　禁用接口，当首次安装 PIX 防火墙时，所有接口默认均是关闭的。需要通

过 interface 命令，不加 shutdown 参数来启动这些接口。

例如，配置 PIX 防火墙以太网接口参数。

```
Pixfirewall(config)#interface ethernet0 auto
Pixfirewall(config)#interface ethernet1 100 full
Pixfirewall(config)#interface ethernet1 100 full shutdown
```



auto 参数表明系统自适应网卡类型；100 full 参数表示使用 100Mbps 以太网全双工通信；shutdown 参数表示关闭这个接口，若启用接口则去掉 shutdown。

3. ip address

在一个接口使用 nameif 和 interface 进行配置后，还需要使用命令 ip address 给这个接口分配一个 IP 地址，用于设备连接使用。其命令语法格式如下所示。

```
ip address if_name ip_address netmask
```

- **if_name** 之前定义的端口描述（如 outside 或 inside）。
- **ip_address** 代表设置的端口 IP 地址。
- **netmask** 用于标识该 IP 地址的子网掩码。

例如，在 PIX 防火墙上配置内外网口的 IP 地址。

```
Pixfirewall(config)#ip address outside 192.168.0.2 255.255.255.0
Pixfirewall(config)#ip address inside 10.0.0.1 255.0.0.0
```

该配置语句表明，PIX 防火墙上用于连接外网的接口 IP 地址为 192.168.0.2，连接内网的接口 IP 地址为 10.0.0.1。

4. nat

nat（网络地址转换），可以将 PIX 防火墙后面的内部网络对外隐藏起来，它通过在转发数据包到外部网络之前，将内部私有 IP 地址转换成外网中公有 IP 地址来完成任务。在 PIX 防火墙中使用 nat 和 global 命令来实现 nat 技术。其命令语法格式如下所示。

```
nat (if_name) nat_id address netmask [timeout hh:mm:ss]
```

- **if_name** 接口名称，对该接口连接的网络进行地址转换。
- **nat_id** 指定用于动态地址转换的全局地址池。
- **address** 要进行地址转换的 IP 地址。
- **hh:mm:ss** 进行地址转换时的超时时间（该参数可选），默认为 3 小时。

例如，在 PIX 防火墙上启用 nat，让内网的所有计算机均可以访问外网、只允许内网中 172.16.5.0 网段的计算机访问外网可配置如下。

```
Pixfirewall(config)#nat (inside) 1 0.0.0.0 0.0.0.0
Pixfirewall(config)#nat (inside) 1 172.16.5.0 255.255.255.0
```

5. global

当某台内部计算机通过防火墙访问外部网络时，可以使用 global 命令和 nat 命令来为这台内部计算机分配一个注册或公共的 IP 地址。如果使用了 nat 命令，就必须使用 global 命令来定义用于转换的 IP 地址。其命令语法格式如下所示。

```
global if_name nat_id global_ip [-global_ip] [netmask global_mask]
```

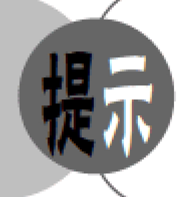
- **if_name**　标识使用全局地址（公共 IP 地址）的外部网络接口名称。
- **nat_id**　标识全局地址池（公共 IP 地址池），要与 nat 命令中 nat_id 相同。
- **global_ip**　一个 IP 地址或一个全局地址范围内的起始 IP 地址。
- **-global_ip**　全局地址范围内的结束 IP 地址。
- **interface**　指定 PAT（端口 NAT）使用接口上 IP 地址。

例如，在 PIX 防火墙上，要实现内网的计算机通过 PIX 防火墙来访问外网时，PIX 防火墙使用 61.144.51.42～61.144.51.48 这一全局地址范围，为访问外网的计算机分配一个全局 IP 地址。

```
Pixfirewall(config)#global (outside) 1 61.144.51.42-61.144.51.48
```

实现内网要访问外网时，PIX 防火墙为访问外网的所有计算机统一分配使用 61.144.51.42 这个单一 IP 地址，其配置命令如下所示。

```
Pixfirewall(config)#global (outside) 1 61.144.51.42
```



若要删除上述在 PIX 防火墙上的配置表项，可在原有命令前添加“no”字段，然后按回车键即可，如 Pixfirewall(config)#no global (outside) 1 61.144.51.42。

6. route

在任何的 PIX 防火墙基础配置中，均需要 route 命令，该命令是为一个接口定义一条静态或默认的路由。其命令语法格式如下所示。

```
route if_name ip_address netmask gateway_ip [metric]
```

- **if_name**　内部或外部网络接口名称。
- **ip_address**　内部或外部网络 IP 地址，使用 0.0.0.0 用于指定一条默认路由。
- **netmask**　指定一个匹配 ip_address 参数的网络掩码。
- **gateway_ip**　指定网络路由器的 IP 地址，即路由的下一跳地址。
- **metric**　表示到 gateway_ip 的跳数，默认为 1。

例如，要在 PIX 防火墙上，定义一条指向边界路由器（IP 地址为 61.144.51.111）的默认路由，其配置命令如下所示。

```
Pixfirewall(config)#route outside 0.0.0.0 0.0.0.0 61.144.51.111 1
```

若内部网络只有一个网段，按照上面那样设置一条默认路由即可，但若内部存在多个网络，则需要配置一条以上的静态路由。如创建两条分别到网络 10.1.1.0 和网络 10.2.0.0 的静态路由，且静态路由的下一跳路由器 IP 地址为 172.16.0.1，其配置命令分别如下所示。

```
Pixfirewall(config)#route inside 10.1.1.0 255.255.255.0 172.16.0.1 1
Pixfirewall(config)#route inside 10.2.0.0 255.255.0.0 172.16.0.1 1
```

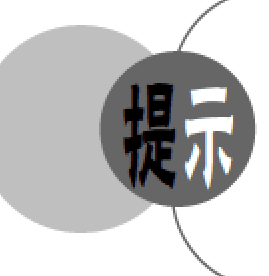
10.2.3 PIX 防火墙的口令恢复

当某用户新购买了一台 PIX 防火墙，欲启动并配置使用时，发现必须输入密码才能进入系统的配置界面。这时，则只能借助于口令恢复技术将该 PIX 防火墙的口令清空。在此，以 PIX 515E 防火墙口令恢复为例。

1. 口令恢复前准备

口令恢复是把从网上下载的相关 PIX IOS 版本的 np**.bin 文件，通过一台 TFTP 服务器发送到 PIX 防火墙操作系统内，来覆盖原有 np**.bin 文件（含密码）的过程。而在进行这个恢复过程之前，需要做以下准备工作。

- 从网上下载相关 PIX IOS 版本的 np**.bin 文件，如与 PIX 515E 防火墙匹配的 np63.bin 文件。
- 在一台计算机上安装 TFTP 服务器程序，并把 np63.bin 放到 TFTP 服务器目录下。
- 将安装 TFTP 服务器程序的计算机作为远程 TFTP 服务器，IP 地址设为 192.168.18.254。
- 使用一条交叉线把 TFTP 服务器的网卡与 PIX 的 ethernet 0 连接起来。
- 使用一条配置专用线（rollover 线）把 TFTP 服务器的 console 口与 PIX 的 console 口连接起来。
- 准备预设 PIX 的 ethernet 0 IP 地址为 192.168.18.111。



该 PIX 515E 防火墙的 np63.bin 文件名称，可通过进入 PIX 防火墙的 monitor> 模式（启动系统后按 Break 键或 Esc 键），输入 show version 并按回车键查看，然后到http://www.cisco.com/warp/public/110/34.html上面下载。

2. 网络拓扑示意图

网络拓扑示意图如图 10-8 所示。

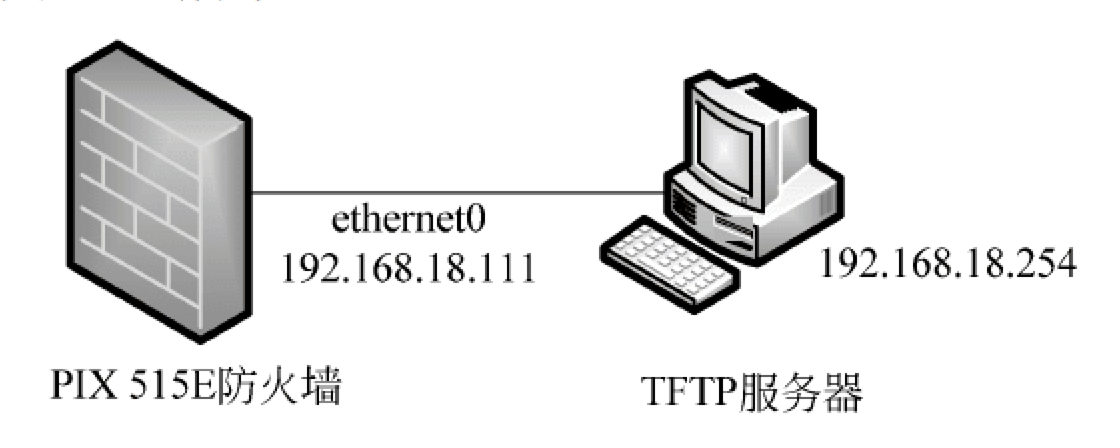


图 10-8 恢复口令拓扑结构图

3. 口令恢复

若进行 PIX 515E 防火墙口令恢复操作，需要启动防火墙系统，显示启动消息后，按 Break 键或 Esc 键进入 monitor>模式。然后，在该模式下所执行的操作及输出界面如下。

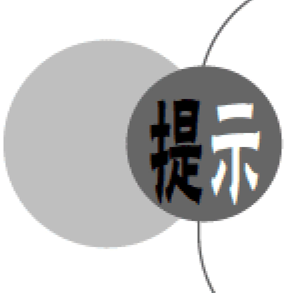
```
monitor> interface 0  （进入 PIX 防火墙的 interface 0 接口）
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7)

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC: 0050.54ff.82b9
monitor> address 192.168.18.111  （为 PIX 的 ethernet 口指定一个 IP 地址，不用输入
掩码）
address 192.168.18.111
monitor> server 192.168.18.254  （为传送 np63.bin 文件的 TFTP 服务器指定 IP 地址，不
用输入掩码）
server 192.168.18.111
monitor> file np63.bin  （指定远程 TFTP 服务器上 np63.bin 的文件名）
file np63.bin
monitor> gateway 192.168.18.254  （指定通过的网关路由器 IP 地址）
gateway 192.168.18.254
monitor> ping 192.168.18.254  （验证 PIX 与远程 TFTP 服务器是否连通）
Sending 5, 100-byte 0xf8d3 ICMP Echoes to 192.168.18.254, timeout is 4 seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor> tftp  （执行 np63.bin 文件的下载传输）
tftp np63.bin@192.168.18.254 via 192.168.18.254........................
Received 92160 bytes

Cisco Secure PIX Firewall password tool (3.0) #0: Tue Aug 22 23:22:19 PDT 2000
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xd8000

Do you wish to erase the passwords? [yn] y  （确定删除口令）
Passwords have been erased.

Rebooting....
```



在上述过程中，ping 192.168.18.254 用来测试到 TFTP 服务器的连通性，若测试不通，则需要仔细检查一下 TFTP 服务器网卡与 PIX 防火墙的连接。另外，在系统删除口令成功后，会自动重启，此时 enable 口令默认为空；但重启后仍提示输入口令，只需按回车键。

10.3　PIX 防火墙的高级配置

在 Cisco PIX 防火墙 IOS 中，除了一些基本配置外，还提供了地址翻译、管道应用、系统日志、攻击防护等高级特性。利用地址翻译允许更改 IP 数据包中的源和目标地址，它通常用

于在网络中使用私有 IP 地址或存在重叠地址的情况；还可以通过管道应用技术，使得内网用户访问外网资源；系统日志和攻击防护功能，提供防火墙安全保护。

10.3.1 PIX 防火墙的翻译

当内部数据通过 PIX 防火墙到达外部时，可以使用 PIX 防火墙转换所有的内部 IP 地址，即 PIX 防火墙的翻译技术（NAT）。从网络安全角度来看，若通过一条特殊的安全策略指定只允许出站流量时（只允许内网访问外网），则转换内网地址是非常安全的；如果内部网络使用的是私有地址，那么经过转换后的源地址必须是在 Internet 上注册过的地址。

当用户尝试从外部建立一个到内部的连接时，这个外部用户将不会成功。除非配置 PIX 防火墙，允许从 Internet 到目标地址是私有地址的会话。

翻译技术有多种类型，对于 PIX 防火墙可配置的有以下几种。

1. 动态 NAT

动态 NAT 可以将一组真实（私有）地址转换成一些全局（公网）地址，这些公网地址均是从一个全局地址的地址池中取出来的，所有公网地址都是在目标网络上可路由的。

当内网计算机向特定目标发起连接时，PIX 防火墙会根据 NAT 规则映射的地址池转换该计算机源地址。在连接没有断开之前，设备会一直维护这个地址转换，当会话终止时，这个地址转换才会被清除。

不过，当同一台计算机发起另一个连接时，不能保证它还能从地址池中获得相同的地址，因为地址池中地址的分配遵循先到先得的原则。所以，鉴于转换后的地址会发生变化，在使用动态 NAT 时，目标网络的用户将无法发起入站连接。动态 NAT 和 PAT 均只能用于单向连接。如图 10-9 所示为动态 NAT 的工作方式。

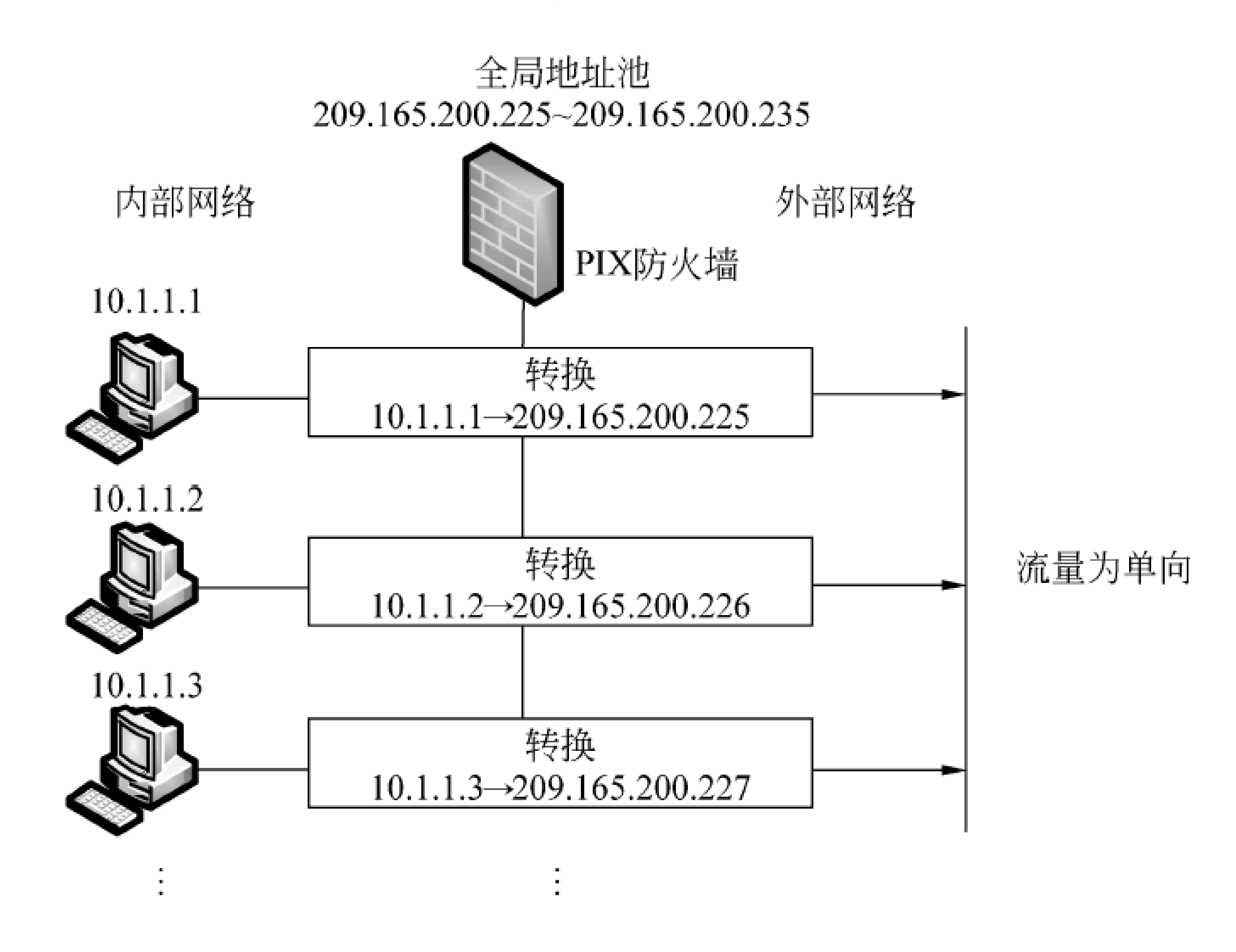


图 10-9 动态 NAT

要实现该 NAT 技术，则需要在 PIX 防火墙上进行如下配置。

```
Pxfirewall(config)#nat (inside) 1 10.1.1.0 255.255.255.0
Pxfirewall(config)#global (outside) 1 209.165.200.225—209.165.200.235
```

2. 动态 PAT

动态 PAT 是把一组真实（私有）地址转换成一个单一的全局地址，然后利用这个映射的全局地址和源端口号的组合，产生唯一的会话。因此，每个会话均有不同源端口号，而所有这些端口号不同的数据包使用的都是同一个全局地址，安全设备（PIX 防火墙）会把源地址和源端口号（第 3 层信息与第 4 层信息的组合）转换成映射的全局地址和一个大于 1024 的唯一端口号。

每个连接所进行的转换均不同，因为这些连接的源端口号各不相同。在连接没有断开之前，设备会一直维护这个地址转换，当会话终止时，这个地址转换才会被清除。但端口转换会在闲置时间超过 30 秒之后超时（超时时间无法进行配置）。

PAT 可以使用单一的映射地址实现转换，因此能够节省可路由的地址资源。安全设备的接口 IP 地址也可以作为 PAT 地址。与动态 NAT 相似的是，在使用动态 PAT 时，目标网络的用户也无法发起入站连接。图 10-10 所示为动态 PAT 的工作方式。

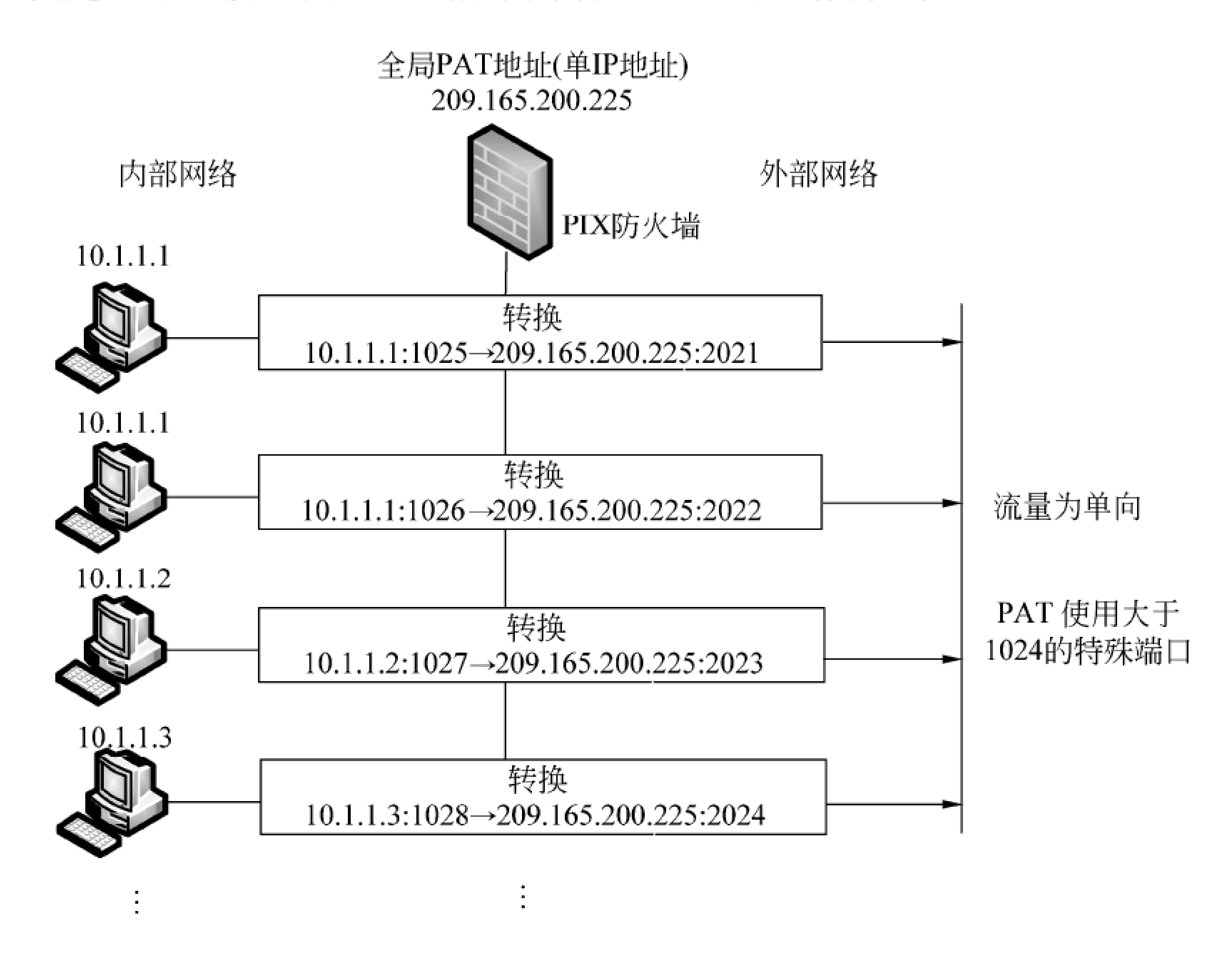


图 10-10　动态 PAT

在 PIX 防火墙上，要想实现动态 NAT 技术则需进行如下配置。

```
Pxfirewall(config)#nat (inside) 1 10.1.1.0 255.255.255.0
Pxfirewall(config)#global (outside) 1 209.165.200.225
```

3. 静态 NAT

静态 NAT 形成的是一个固定不变的（一对一）转换，将真实（私有）地址映射成全局（公网）地址。每个连续的连接通过静态 NAT 都可以拥有一个固定的转换规则。由于映射的地址不变，所以目标网络的用户可以向被转换计算机发起连接。

使用 static 命令可以为一个较高安全级别接口上的计算机地址和一个较低安全级别接口上的计算机地址建立一个永久性的关联。静态的 NAT 和 PAT 均可用于双向连接。图 10-11 所示为一个静态 NAT 的工作方式。

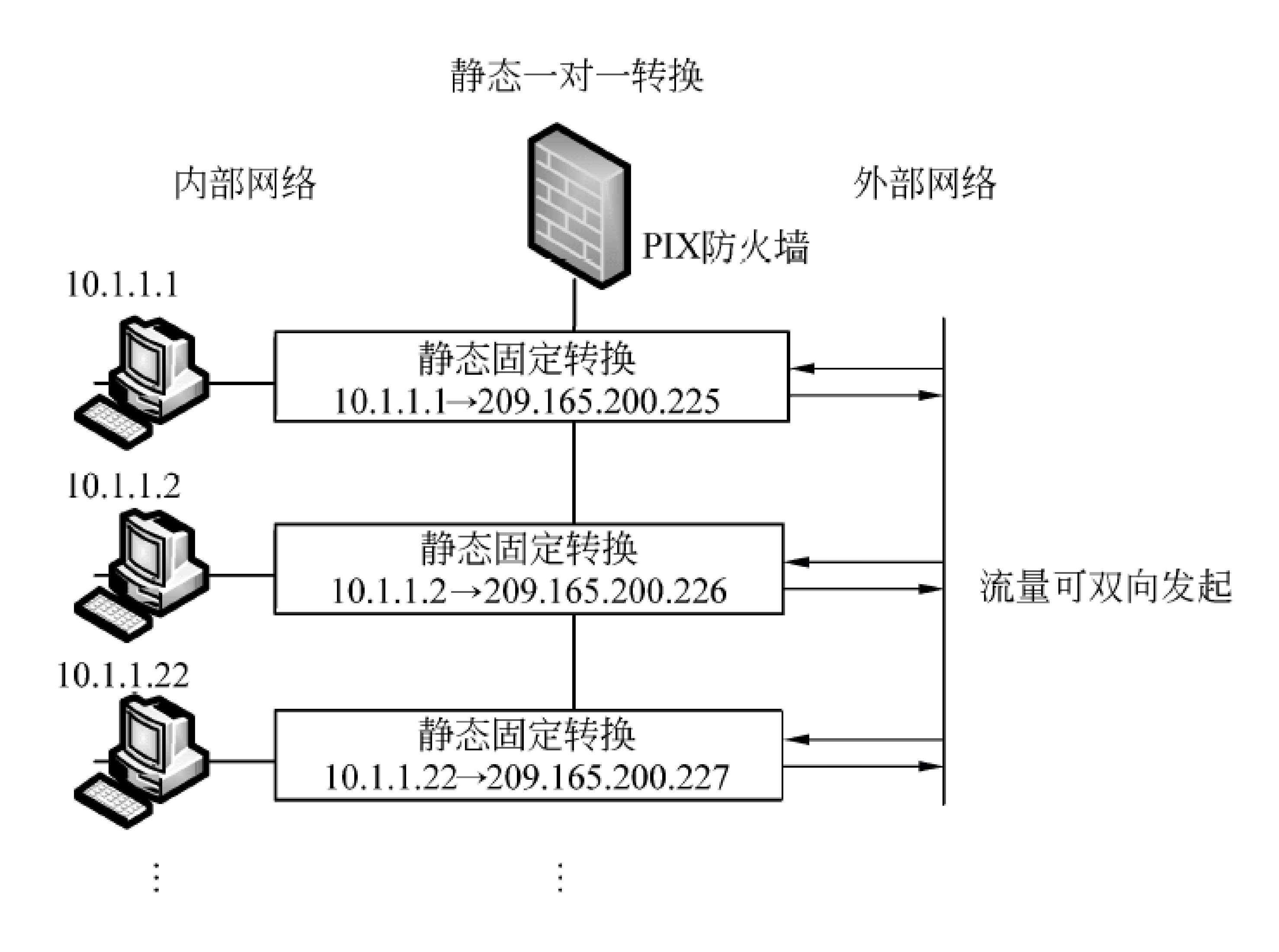


图 10-11 静态 NAT

在 PIX 防火墙上，实现该静态 NAT 技术则需进行如下配置。

```
Pixfirewall(config)#static (inside,outside) 209.165.200.225 10.1.1.1 netmask
255.255.255.255
Pixfirewall(config)#static (inside,outside) 209.165.200.226 10.1.1.2 netmask
255.255.255.255
Pixfirewall(config)#static (inside,outside) 209.165.200.227 10.1.1.22 netmask
255.255.255.255
```

例如，配置内部 NAT（一对一）静态转换，将一个内部 IP 地址（10.1.1.1）到一个外部 IP 地址（209.165.200.1）配置为静态 NAT 转换（固定转换），需输入以下命令。

```
Pixfirewall(config)#static (inside,outside) 209.165.200.1 10.1.1.1 netmask
255.255.255.255
```

配置外部 NAT（一对一）静态转换，利用静态映射将外部地址（209.165.200.15）到内部地址（209.165.200.6）配置为一个外部 NAT 转换（固定转换），需输入以下命令。

```
Pixfirewall(config)#static (outside,inside) 209.165.200.15 209.165.200.6
netmask 255.255.255.255
```

配置内部 NAT 把整个子网执行（一对一）静态转换，将一个具有 24 位子网掩码的子网（一对一，计算机对计算机）配置为一个静态的映射（固定转换），需输入以下命令。

```
Pixfirewall(config)#static (inside,outside) 209.165.200.0 10.1.1.0 netmask
255.255.255.0
```

4. 静态 PAT

静态 PAT 与静态 NAT 有些相似，它们的区别在于静态 PAT 可以为私有地址和转换后的地址指定第 4 层端口信息。

若 TFTP、HTTP 和 SMTP 等服务在本地网络的不同服务器上时，如果想要为公网用户提供单一的地址去访问这些服务，使用 PAT 是非常合适的。此时，需要为所有服务器定义多个静态语句，将这些服务器各自的真正 IP 地址映射到同一公有 IP 地址和不同端口。图 10-12 所示为一个静态 PAT 的例子。

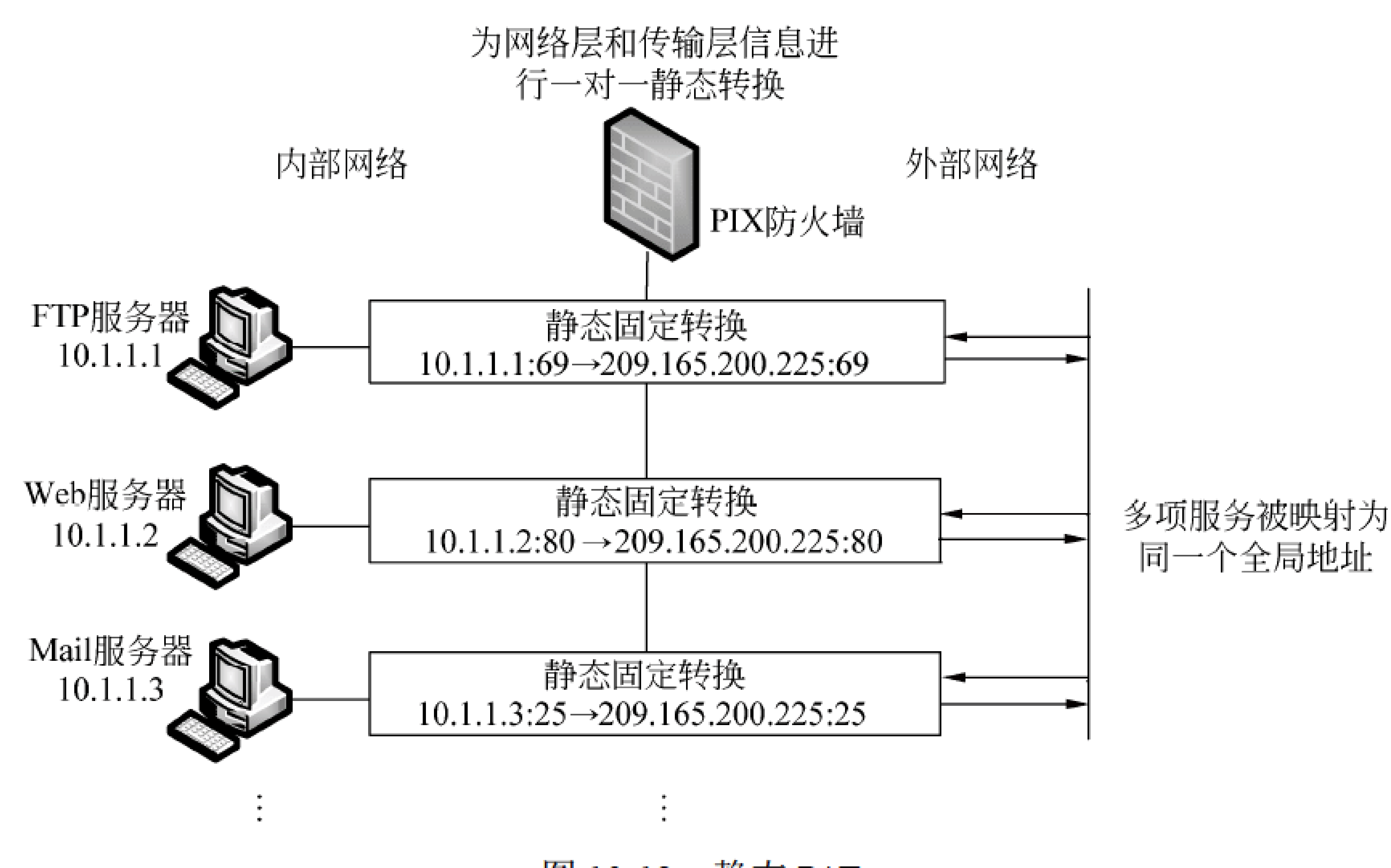


图 10-12　静态 PAT

在 PIX 防火墙上，要实现该 PAT 实例目的，则需进行如下配置。

```
Pixfirewall(config)#static (inside,outside) udp 209.165.200.225 tftp 10.1.1.1
tftp netmask
255.255.255.255
Pixfirewall(config)#static (inside,outside) tcp 209.165.200.225 http 10.1.1.2
http netmask
255.255.255.255
Pixfirewall(config)#static (inside,outside) tcp 209.165.200.225 smtp 10.1.1.3
smtp netmask
255.255.255.255
```

10.3.2　PIX 防火墙的管道应用

尽管大多数的连接是从高安全级别接口到低安全级别的接口，但有时也有来自低安全级

别到高安全级别接口的连接。而对于低安全级别接口到高安全级别接口的连接，则可以使用 static（静态地址翻译）和 conduit（设置管道）命令。PIX 防火墙管道应用网络拓扑图，如图 10-13 所示。

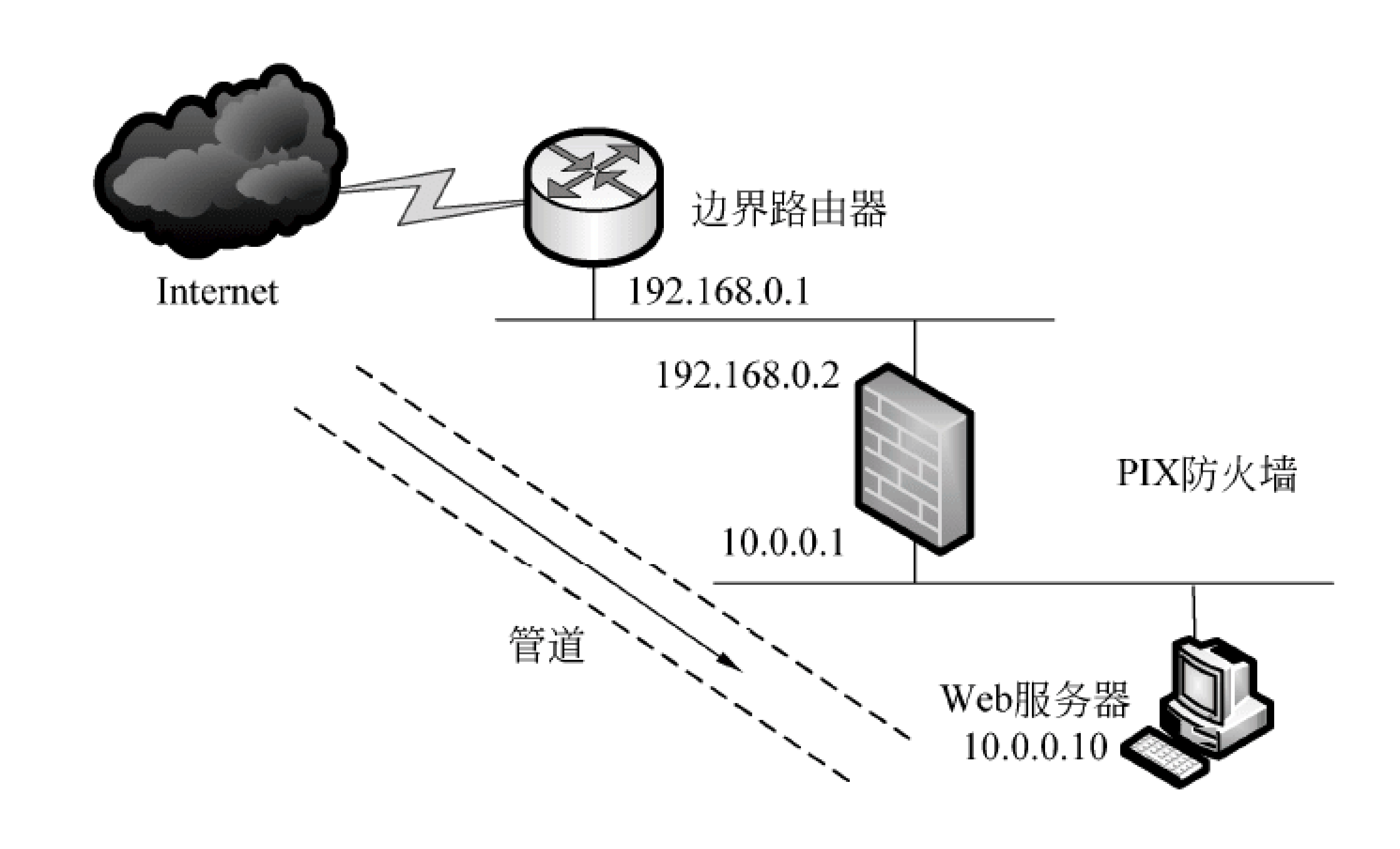


图 10-13 PIX 防火墙管道应用

由于 static 命令允许在一个特殊的内部地址和一个全局地址之间，建立一个永久的映射关系，这样将为低安全级别的接口访问高安全级别的接口设置一个管道，从而实现内网访问外网的目的。

然而，即使使用 static 命令创建一个内部 IP 地址到全局地址的静态映射关系，但 PIX 防火墙的安全算法仍然会堵塞从外部接口（安全级别较高）到内部接口的连接。此时，则需要通过 conduit 命令解决该问题，因为 conduit 命令的应用，能够在 PIX 防火墙的 ASA 上允许接口之间的流量经过。

conduit 命令能够实现，从 PIX 防火墙的外部到内部网络上某台计算机的 TCP 或 UDP 服务的连接，即形成连接管道，且可多达 8000 个。另外，还可使用 no conduit 命令来删除一个管道。conduit 命令的语法如下所示。

```
conduit permit |deny protocol global_ip global_mask [operator port (port)]
foreign_ip foreign_mask [operator port (port)]
```

- **permit|deny** 允许|拒绝访问。
- **global_ip** 指之前由 global 或 static 命令定义的全局 IP 地址，若 global_ip 为 0，则可使用 any 代替 0，若 global_ip 代表一台计算机，则可利用 host 命令参数。
- **port** 指定内部服务所用的端口，可使用服务名称或端口数字来配置，如 WWW 使用 80，SMTP 使用 25 等。
- **protocol** 指建立连接所使用的协议，如 TCP、UDP、ICMP 等。
- **foreign_ip** 表示可访问 global_ip 的外部 IP。对于所有或任意计算机，可使用 any 表示，若 foreign_ip 代表一台计算机，则用 host 命令参数。

若要在 PIX 防火墙上进行如下管道应用设置时，其代表的含义分别如下所述。

```
Pixfirewall(config)#conduit permit tcp host 192.168.0.8 eq www any
```

表示允许任何外部计算机对全局地址为 192.168.0.8 的计算机进行 http 访问。其中使用 eq 和一个端口（www）来允许或拒绝对该端口的访问。eq ftp 就代表允许或拒绝只对 ftp 服务器的访问。

```
Pixfirewall(config)#conduit deny tcp any eq ftp host 61.144.51.89
```

表示不允许外部 IP 地址为 61.144.51.89 的计算机，对任何全局地址进行 ftp 访问。

```
Pixfirewall(config)#conduit permit icmp any any
```

表示允许 ICMP 消息可以在内部网络和外部网络之间双向传递。另外，假设内网用户可以 ping 外部计算机时，那么必须为 ICMP 的 echo reply（ICMP 应答）创建一个 ICMP 通道。如 Pixfirewall(config)#conduit permit icmp any any echo-reply。

```
PixfireWall(config)#static (inside,outside) 61.144.51.66 192.168.0.4
PixfireWall(config)#static permit tcp host 61.144.51.66 eq www any
```

该例子说明 static 和 conduit 的关系。192.168.0.4 代表内网的一台 Web 服务器，要实现外网用户能够通过 PIX 防火墙得到 Web 服务，因此先做 static 静态映射（192.168.0.4—>61.144.51.66），然后利用 conduit（通道）命令，允许任何外网计算机对全局地址 61.144.51.66 进行 http 访问。

10.3.3　PIX 防火墙系统日志

系统日志用来记录系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的事件。用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。

通常，PIX 防火墙在记录和显示日志时，将会指定系统日志消息等级为一个数字或字符串（默认等级为 3）；还可以采用手动方式指定其日志消息等级（level），来表示想要显示该等级和低于该等级的系统日志消息。例如，日志等级为 5 时，则系统日志将显示 0～5 级的消息。

PIX 防火墙系统中，可用于指定日志等级的数字或字符串值，如表 10-1 所示。

表 10-1　日志级别及显示形式

级别（数字）	级别（字符串）	代表含义
0	emergencies	系统不可用消息
1	alerts	立即采用行动
2	critical	关键状态
3	errors	出错消息
4	warrings	警告消息
5	notifications	正常但有特殊意义的状态
6	informational	信息消息
7	debugging	调试消息、FTP 命令及 WWW URL 记录

在一般情况下，PIX 防火墙的日志功能是禁用的。为了启动日志功能，需要使用 logging on

命令，并把日志发送到某一台日志服务器上。其配置过程如下所示。

```
Pixfirewall(config)#logging on  （启动日志功能）
Pixfirewall(config)#logging 192.168.0.1  （日志服务器的 IP 地址）
Pixfirewall(config)#logging facility local 1  （facility 标识，RFC3164 规定的本地设备标识为 local   0~local 7）
Pixfirewall(config)#logging trap errors（指定日志服务级别，可输入"？"查看详细内容）
Pixfirewall(config)#logging source-interface ethernet 0（指定日志发出时用的源IP 地址）
Pixfirewall(config)#service timestamps log datetime localtime  （设置日志记录时的时间间隔）
Pixfirewall(config)#show logging  （检查日志）
```

另外，在 PIX 防火墙上还可对系统日志进行其他一些设置，如日志系统缓冲区级别、缓冲区大小、历史记录大小及如何关闭日志功能等，它们的配置方法分别如下所示。

```
Pixfirewall(config)#logging buffered 5  （设置缓冲区级别）
Pixfirewall(config)#logging buffered 5000  （设置缓冲区大小）
Pixfirewall(config)#logging history 20  （设置历史记录大小，默认为 10）
Pixfirewall(config)#no logging  （禁用系统日志功能）
```

10.3.4　PIX 防火墙高级协议处理

在内网与外网之间由防火墙建立连接中，当外部用户访问内网时，每个入站数据包都将会由防火墙对其进行检测，这也是所有防火墙最基本的功能（主要对网络层进行检测）。

不过，随着攻击技术的不断发展，为了防止非法用户以高级协议（如传输层协议、应用层协议）为攻击点进行入侵，逐步推出了基于传输层、应用层实施监控的防火墙产品，Cisco PIX 防火墙在这一点就有很大的突破。因为，它除了对网络层进行检测外，还支持状态化监控和应用层协议监控两种技术，保护网络的安全。

1. 状态化监控

对于 PIX 防火墙来说，任何一个入站数据包都将由它根据自适应安全算法和连接状态信息进行监控，以此决定是要放行还是要丢弃这个数据包。

如果到达的数据包是新建连接的一部分，自适应安全算法会根据访问控制列表（ACL）及其他常规任务（如路由表）来判断是放行还是丢弃该数据包。此时，PIX 状态化防火墙中会话管理路径会按照如下顺序检查数据包的状态。

- 检查访问列表（ACL）。
- 查看路由表。
- 指派 NAT 转换。
- 建立会话的“快速路径”。
- 将数据包交给检测程序，来检查它的负载以实现应用层监控。

如果到达的数据包属于一个已经建立的连接，自适应安全算法不会重新对这个数据包进行检查，它会通过快速路径双向穿越防火墙的已建立连接表中匹配这个数据包。快速路径会

进行如下检查。

- IP 校验和验证。
- 查看会话。
- 检查 TCP 序列号。
- 根据已建立的会话进行 NAT 转换。
- 核对网络层和传输层数据报头。

2. 应用层协议监控

除了上面提到的状态化监控功能外，自适应安全算法还增加了应用层智能监控功能，它可以检查并且制止一些应用层协议的攻击。

应用层协议监控功能，可以对数据包的 IP 头部和负载（数据）部分的内容进行检查，以此实现对应用层协议流量（如 HTTP）的深度监控。传统的防火墙最多只能维护传输层的会话信息，但 Cisco PIX 防火墙（还有其他安全设备）防御功能上了一个台阶，进而可以对数据包的应用层负载信息进行监控。

由于 Cisco PIX 防火墙能够了解应用层的信息，也就可以对数据包的负载部分进行深度监控，以探测到一切恶意的行为。如图 10-14 所示，当防火墙收到一个常见应用层协议的数据包（如 HTTP）时，它会根据相应的应用层协议来对这个数据包进行检查；查看这个数据包的操作行为是否符合 RFC 标准，以此判断这个数据包是否存在恶意的企图。

如果这个数据包是经过恶意伪装的，那么设备就会发现它的操作和行为不符合 RFC 标准，于是这个数据包将会被设备阻塞。而如果使用传统的访问列表，这些数据包将会被设备放行，因为访问控制列表只能检查数据包的网络层和传输层信息。

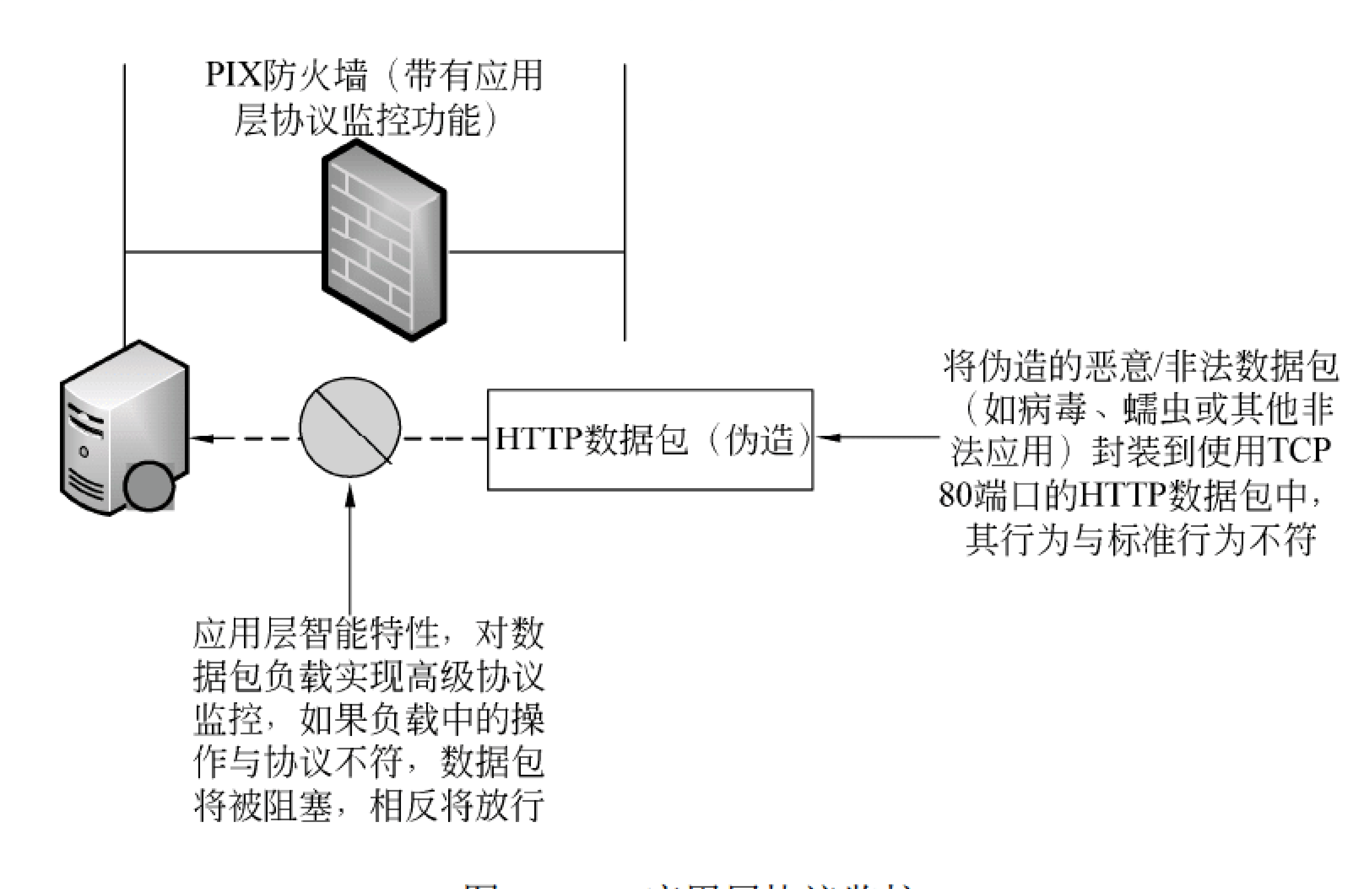


图 10-14　应用层协议监控

许多网络攻击采取的都是嵌入式的方法，即将恶意的流量封装到常用的应用层协议中来发起攻击，而具备应用层监控功能的 PIX 防火墙，就可以采用以上监控技术保护网络免受许多这类攻击的侵袭。

10.3.5 PIX 防火墙攻击防护

攻击防护功能是防火墙的重要特性之一，通过分析报文的内容特征和行为特征判断报文是否具有攻击特性，并且对攻击行为采取措施以保护网络计算机或者网络设备。

防火墙的攻击防护功能，能够检测拒绝服务型、扫描窥探型、畸形（伪造）报文型等多种类型的攻击，并对攻击采取合理的防范措施。攻击防护的具体功能包括黑名单过滤、报文攻击特征识别、流量异常检测和入侵检测统计。

随着网络技术的普及和应用的多样化与复杂化，出现的攻击行为越来越多，使得各种网络病毒泛滥，加剧网络被攻击的危险。目前，Internet 上常见的网络安全威胁分为以下三类。

❑ **DoS 攻击**

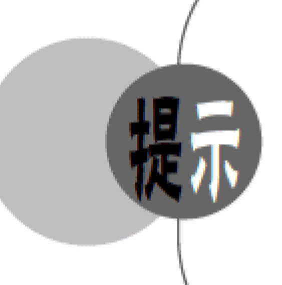
DoS 攻击是利用大量的数据包攻击目标系统，使目标系统无法接受正常用户的请求，或者使目标主机挂起不能正常工作，其主要攻击方式有 SYN Flood、Fraggle 等。DoS 攻击和其他类型的攻击不同之处在于，攻击者并不是去寻找进入目标网络的入口，而是通过扰乱目标网络的正常工作来阻止合法用户访问网络资源。

❑ **扫描窥探攻击**

扫描窥探攻击利用 ping 扫描（包括 ICMP 和 TCP）标识网络上存在的活动计算机，从而可以准确定位潜在目标的位置；利用 TCP 和 UDP 端口扫描检测出目标操作系统和启用的服务类型。攻击者通过扫描窥探，能够大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步入侵目标系统作好准备。

❑ **畸形报文攻击**

畸形报文攻击是通过向目标系统发送有缺陷的 IP 报文，如分片重叠的 IP 报文、TCP 标志位非法的报文，使得目标系统在处理这些 IP 报文时崩溃，给目标系统带来损失。主要的畸形报文攻击有 Ping of Death、Teardrop 等。



在多种网络攻击类型中，DoS 攻击是最常见的一种，因为这种攻击方式对攻击技能要求不高，攻击者可以利用各种开放的攻击软件实施攻击行为，所以 DoS 攻击的威胁逐步增大。成功的 DoS 攻击会导致服务器性能急剧下降，造成正常客户访问失败；同时，提供服务的企业的信誉也会蒙受损失，而且这种危害是长期性的。

PIX 防火墙，能够利用有效的攻击防范技术，主动防御各种常见的网络攻击，保证网络在遭受越来越频繁的攻击的情况下能够正常运行，从而实现防火墙的整体安全解决。在 PIX 防火墙系统中，常见攻击及防护方式如下所述。

1. 地址扫描攻击及防护

运用 ping 类型的程序探测目标地址，对此作出响应的系统表示其存在，该探测可以用来确定哪些目标系统确实存在并且是连接在目标网络上的。也可以使用 TCP/UDP 报文对一定地址发起连接（如 TCP ping），通过判断是否有应答报文来探测目标网络上有哪些系统是开放的。

检测进入 PIX 防火墙的 ICMP、TCP 和 UDP 报文，统计从同一个源 IP 地址发出报文的不同目的 IP 地址个数。如果在一定的时间内，目的 IP 地址的个数达到设置的阈值，则直接丢弃报文，并记录日志，然后根据配置决定是否将源 IP 地址加入黑名单。

2. 端口扫描攻击及防护

端口扫描攻击通常使用一些软件，向目标主机的一系列 TCP/UDP 端口发起连接，根据应答报文判断主机是否使用这些端口提供服务。

利用 TCP 报文进行端口扫描时，攻击者向目标主机发送连接请求（TCP SYN）报文，若请求的 TCP 端口是开放的，目标主机回应一个 TCP ACK 报文，若请求的服务未开放，目标主机回应一个 TCP RST 报文，通过分析回应报文是 ACK 报文还是 RST 报文，攻击者可以判断目标主机是否启用了请求的服务。

利用 UDP 报文进行端口扫描时，攻击者向目标主机发送 UDP 报文，若目标主机上请求的目的端口未开放，目标主机回应 ICMP 不可达报文，若该端口是开放的，则不会回应 ICMP 报文，通过分析是否回应了 ICMP 不可达报文，攻击者可以判断目标主机是否开放了端口。这种攻击通常在判断出目标主机开放了哪些端口之后，将会针对具体的端口进行更进一步的攻击。

检测进入 PIX 防火墙的 TCP 和 UDP 报文，统计从同一个源 IP 地址发出报文的不同目的端口个数。如果在一定的时间内，端口个数达到设置的阈值，则直接丢弃报文，并记录日志，然后根据配置决定是否将源 IP 地址加入黑名单。

3. Land 攻击及防护

Land 攻击利用 TCP 连接建立的三次握手功能，通过将 TCP SYN 包的源地址和目标地址都设置成某一个受攻击者的 IP 地址，导致受攻击者向自己的地址发送 SYN ACK 消息。这样，受攻击者在收到 SYN ACK 消息后，就会又向自己发送 ACK 消息，并创建一个空 TCP 连接，而每一个这样的连接都将保留直到超时。

因此，如果攻击者发送了足够多的 SYN 报文，就会导致被攻击者系统资源大量消耗。各种系统对 Land 攻击的反应不同，UNIX 系统将崩溃，Windows 系统会变得极其缓慢。

存在此攻击时，PIX 防火墙将检测每一个 IP 报文的源地址和目标地址，若两者相同，或者源地址为环回地址 127.0.0.1，则根据用户配置选择对报文进行转发或拒绝接收，并将该攻击记录到日志。

4. Smurf 攻击及防护

简单的 Smurf 攻击是向目标网络计算机发 ICMP 应答请求报文，该请求报文的目标地址设置为目标网络的广播地址，这样目标网络的所有计算机都对此 ICMP 应答请求做出答复，导致网络阻塞。

高级的 Smurf 攻击是将 ICMP 应答请求报文的源地址改为目标计算机的地址，通过向目标计算机持续发送 ICMP 应答请求报文最终导致其崩溃。

若存在该攻击时，PIX 防火墙将检查 ICMP 应答请求报文的目标地址是否为子网广播地址

或子网的网络地址，如果是，则根据用户配置选择对报文进行转发或拒绝接收，并将该攻击记录到日志。

5. Fraggle 攻击及防护

它类似于 Smurf 攻击，只是它利用 UDP 应答报文而不是 ICMP 报文。攻击者向某子网广播地址发送源地址为目标网络或目标计算机的 UDP 报文，目的端口号使用 7（echo 服务）或 19（Chargen 服务）。该子网内启用 echo 服务或者 Chargen（一种仅仅发送字符的服务）服务的每个计算机都会向目标网络或目标计算机发送响应报文，从而引发大量无用的响应报文，导致目标网络的阻塞或目标计算机的崩溃。

检查进入 PIX 防火墙的 UDP 报文，如果报文的目的端口号为 7 或 19，则根据用户配置选择对报文进行转发或拒绝接收，并将该攻击记录到日志，否则允许通过。

6. SYN Flood 攻击及防护

SYN Flood 攻击通过伪造一个 SYN 报文向服务器发起连接，其源地址是伪造的或者一个不存在的地址。服务器在收到该报文后发送 SYN ACK 报文应答，由于攻击报文的源地址不可达，因此应答报文发出去后，不会收到 ACK 报文，造成一个半连接。如果攻击者发送大量这样的报文，会在被攻击计算机上出现大量的半连接，从而消耗其系统资源，使正常的用户无法访问。

遭受该攻击时，可将 PIX 防火墙作为客户端与服务器通信的中继，当客户端发起连接时，防火墙并不把 SYN 报文传递给服务器，而是自己向客户端发送 SYN ACK 报文，之后如果防火墙收到客户端的确认报文，才会与服务器进行连接。

7. ICMP Flood 攻击及防护

ICMP Flood 攻击通过短时间内向特定目标系统发送大量的 ICMP 消息（如执行 ping 程序）来请求其回应，致使目标系统忙于处理这些请求报文而不能处理正常的网络数据报文。

此时，PIX 防火墙可通过智能流量检测技术，检测通向特定目的地址的 ICMP 报文速率，如果报文速率超过阈值上限，则认为攻击开始，就根据用户的配置选择丢弃或者转发后续连接请求报文，同时将该攻击记录到日志。当速率低于设定的阈值下限后，检测到攻击结束，正常转发后续连接请求报文。

8. UDP Flood 攻击及防护

其攻击原理与 ICMP Flood 攻击类似，攻击者在短时间内通过向特定目标发送大量的 UDP 消息，导致目标系统负担过重而不能处理正常的数据传输任务。

PIX 防火墙遭遇该攻击时，可通过智能流量检测技术，检测通向特定目标地址的 UDP 报文速率，如果报文速率超过阈值上限，则检测到攻击开始，就根据用户的配置选择丢弃或者转发后续连接请求报文，同时将该攻击记录到日志。当速率低于设定的阈值下限后，检测到攻击结束，正常转发后续连接请求报文。

10.4　操作实例

10.4.1　操作实例——PIX 防火墙的基本配置

PIX 防火墙应用安全算法，拒绝未经允许的数据包，实现动态，静态地址映射，有效屏蔽内部网络，通过管道技术，控制内外部各种资源的访问。

1．实例目的

- 显示运行配置文件。
- 命名接口名称。
- 设置接口安全级别。
- 设置接口 IP 地址。

2．实例步骤

（1）在用户模式下输入 enable（进入特权模式）命令，并按回车键，如图 10-15 所示。

（2）在特权模式下输入 configure terminal（进入全局配置模式）命令，并按回车键，如图 10-16 所示。

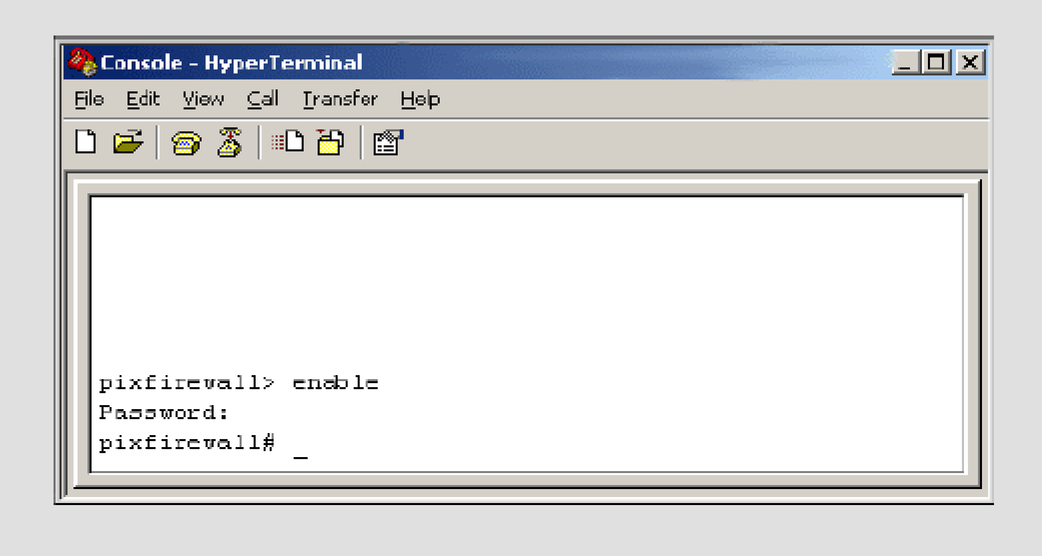


图 10-15　进入特权模式

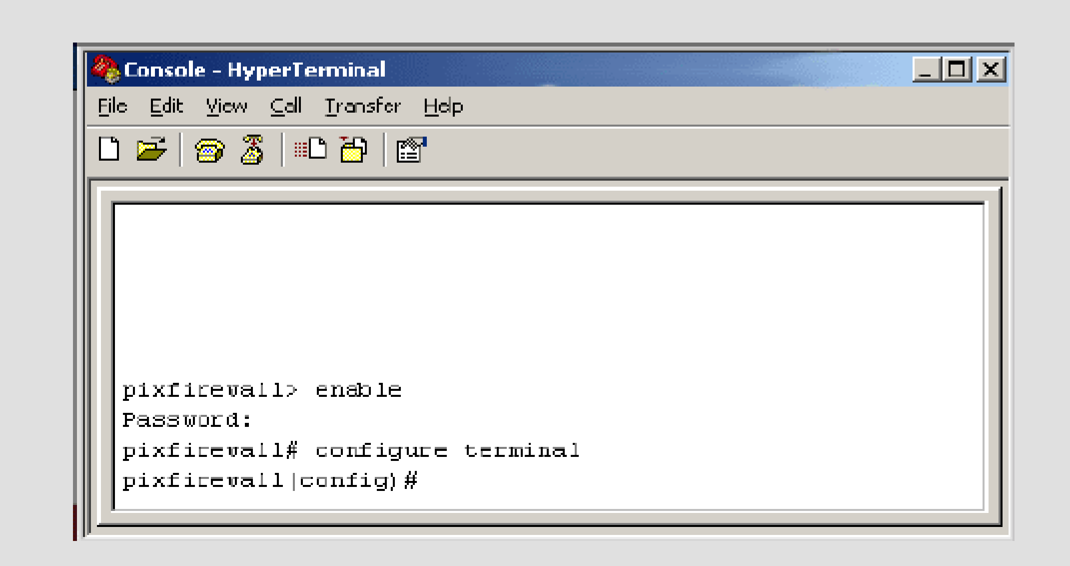


图 10-16　进入全局配置模式

（3）在全局配置模式下输入 write terminal（显示运行配置文件）命令，并按回车键，如图 10-17 所示。

（4）在全局配置模式下输入 hostname KPIX（命名防火墙）命令，并按回车键，如图 10-18 所示。

（5）在全局配置模式下输入 nameif e2 dmz security50（设置 e2 接口名字为 dmz，安全级别为 50）命令，并按回车键，如图 10-19 所示。

（6）在全局配置模式下输入 show nameif（查看接口信息）命令，并按回车键，如图 10-20 所示。

（7）在全局配置模式下输入 interface e0 100 full（设置端口为 100Mbps 全双工通信）命令，

并按回车键，如图 10-21 所示。

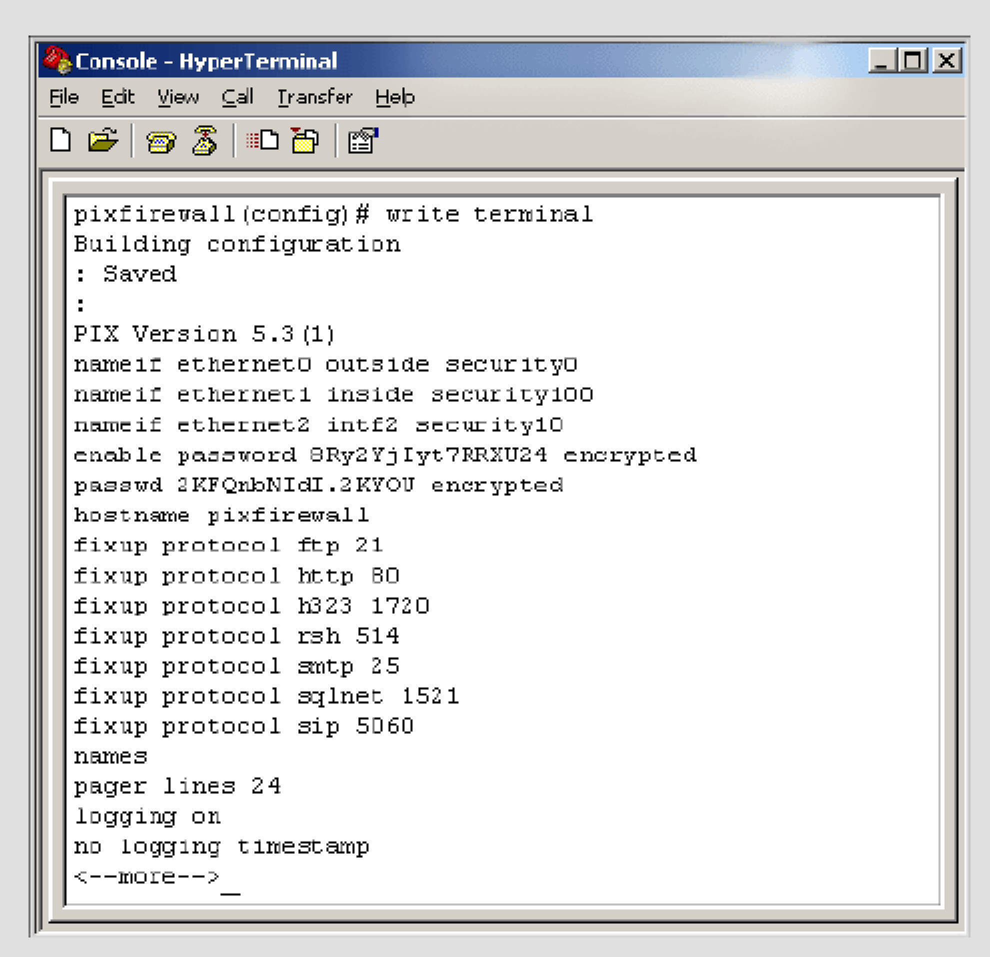


图 10-17　显示运行配置文件



图 10-18　给防火墙命名

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02::3 0:05:0
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
pixfirewall(config)# hostname KPIX
KPIX(config)# nameif ?
usage: [no] nameif <hardware_id> <if_name> <
KPIX(config)# nameif e2 dmz security50
KPIX(config)#
```

图 10-19　命名接口名称并设置安全级别

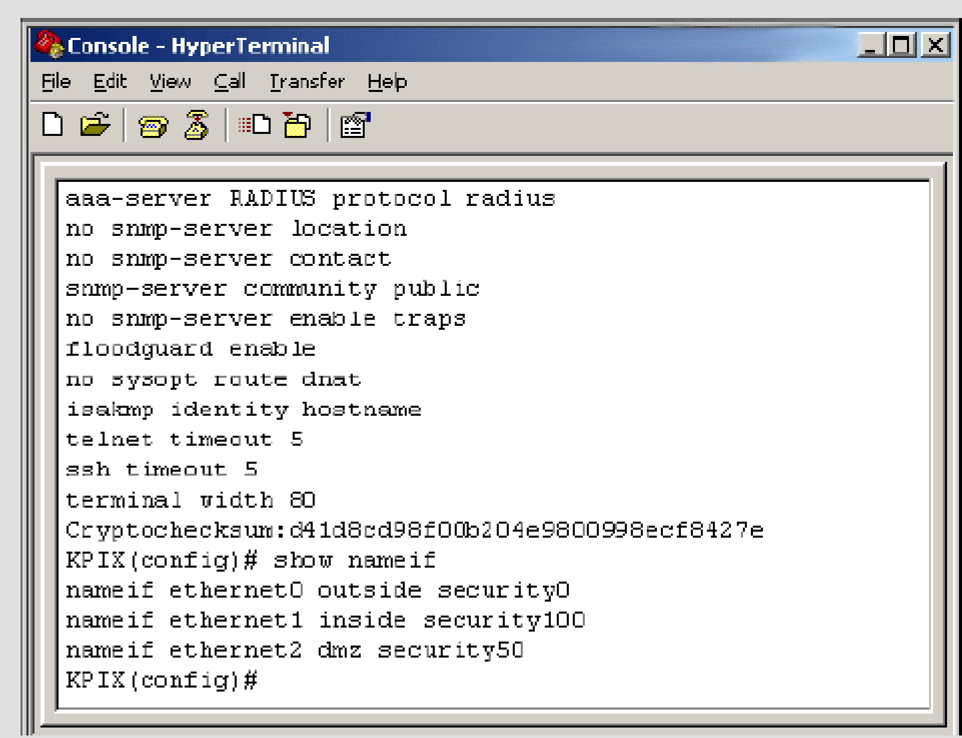


图 10-20　查看接口信息

（8）在全局配置模式下输入 write memory（保存配置）命令，并按回车键，如图 10-22 所示。

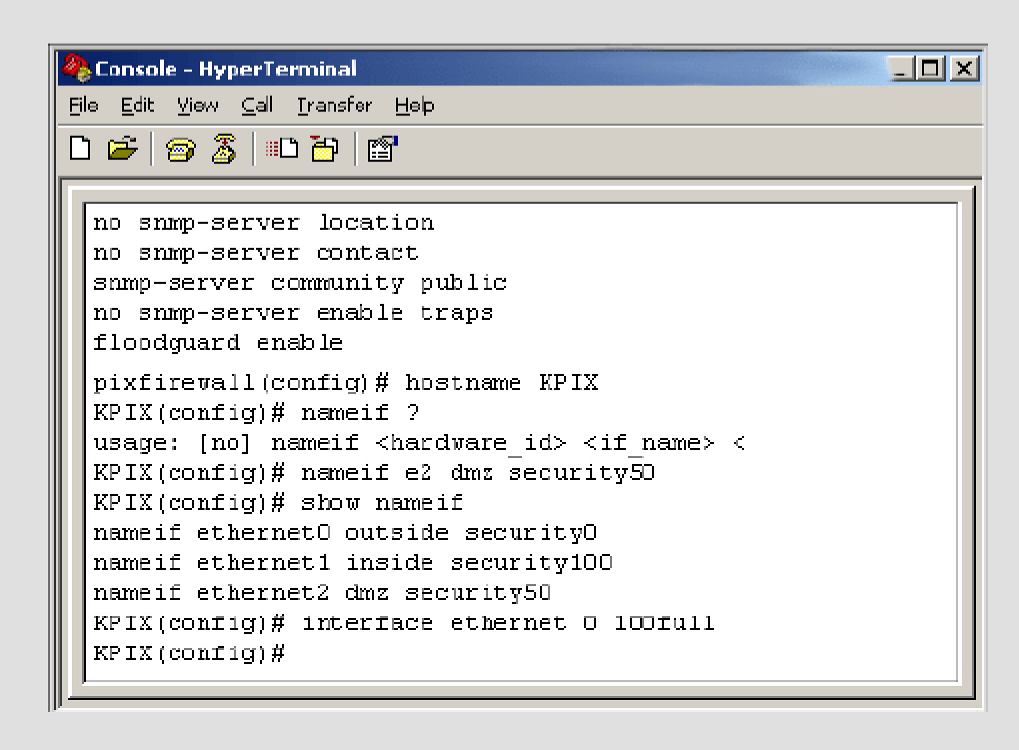


图 10-21　设置接口类型为全双工通信

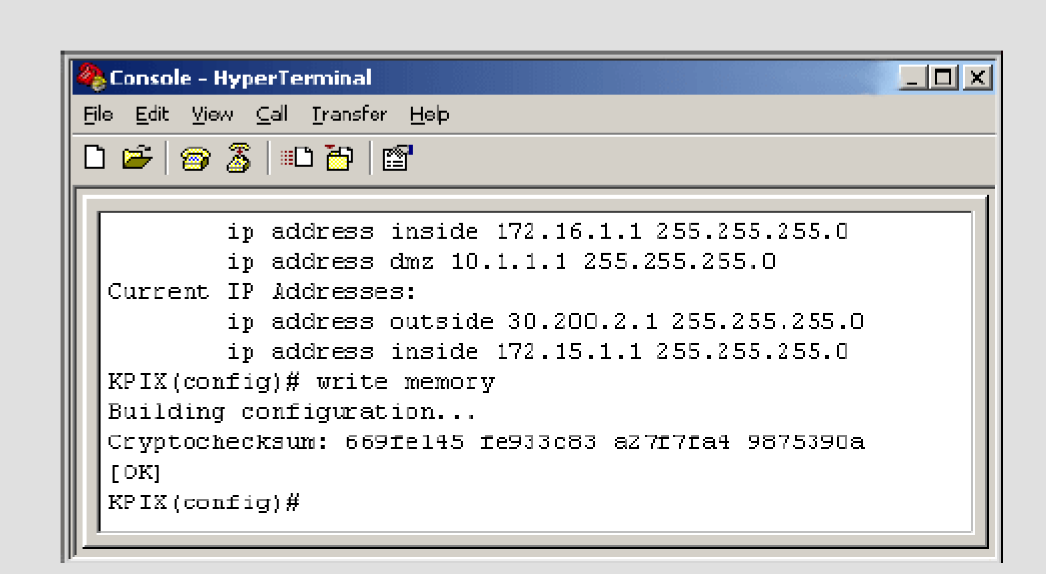


图 10-22　保存配置

10.4.2　操作实例——PIX 防火墙的 NAT 配置

NAT 通过在转发数据包到外部网络之前，将内部 IP 转换为全球公认的 IP 地址，实现将 PIX 后面的内部网络对外隐藏起来的任务。

1. 实例目的

- ❑ 配置接口名称。
- ❑ 配置接口安全等级。
- ❑ 创建转换地址池。

2. 实例步骤

（1）在非特权模式下输入 enable（进入特权模式）命令，并按回车键，如图 10-23 所示。

（2）在特权模式下输入 configure terminal（进入配置模式）命令，并按回车键，如图 10-24 所示。

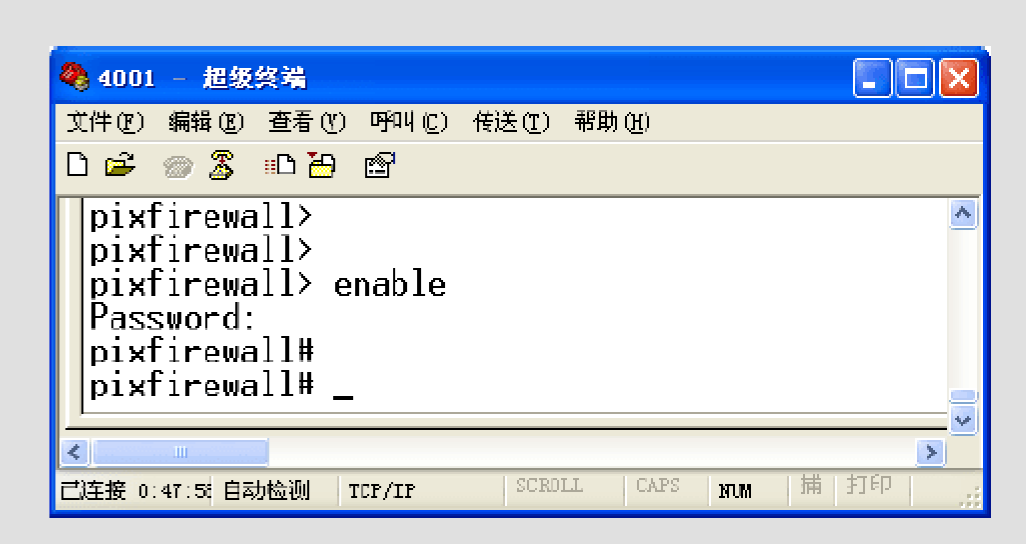


图 10-23　进入特权模式



图 10-24　进入配置模式

（3）在配置模式下输入 interface e0（进入 e0 接口）命令，并按回车键，如图 10-25 所示。

（4）在接口模式下输入 speed auto（配置 e0 接口为自适应接口）命令，并按回车键，如图 10-26 所示。



图 10-25　进入 e0 接口



图 10-26　配置 e0 接口为自适应接口

（5）在接口模式下输入 nameif inside（配置 e0 接口为内网接口）命令，并按回车键，如图 10-27 所示。

（6）在接口模式下输入 security-level 100（配置 inside 接口安全级别为 100）命令，并按

回车键，如图 10-28 所示。



图 10-27　配置 e0 接口为内网接口

```
pixfirewall(config-if)#
pixfirewall(config-if)#
pixfirewall(config-if)#
pixfirewall(config-if)# nameif inside
pixfirewall(config-if)# security-level 100
pixfirewall(config-if)#
pixfirewall(config-if)#
pixfirewall(config-if)#
```

图 10-28　配置 inside 接口安全级别

（7）在接口模式下输入 ip address 192.168.1.1 255.255.255.0（配置 e0 接口 IP 地址）命令，并按回车键，如图 10-29 所示。

（8）在接口模式下输入 interface e1（进入 e1 接口）命令，并按回车键，如图 10-30 所示。

```
pixfirewall(config-if)# speed auto
pixfirewall(config-if)# security-level 100
pixfirewall(config-if)#
pixfirewall(config-if)#
pixfirewall(config-if)# ip add 192.168.10.1
255.255.255.0
pixfirewall(config-if)#
pixfirewall(config-if)# _
```

图 10-29　配置 e0 接口 IP 地址



图 10-30　进入 e1 接口

（9）在接口模式下输入 speed auto（配置 e1 接口为自适应接口）命令，并按回车键，如图 10-31 所示。

（10）在接口模式下输入 nameif outside（配置 e1 接口为外网接口）命令，并按回车键，如图 10-32 所示。



图 10-31　配置 e1 接口为自适应接口



图 10-32　配置 e1 接口为外网接口

（11）在接口模式下输入 security-level 0（配置 outside 接口安全级别为 0）命令，并按回车键，如图 10-33 所示。

（12）在接口模式下输入 ip address 219.140.164.26 255.255.255.0 命令，并按回车键，如图

10-34 所示。



图 10-33　配置 e0 接口安全级别



图 10-34　配置 e1 接口 IP 地址

（13）在接口模式下输入 exit（退出接口模式）命令，并按回车键，如图 10-35 所示。

（14）在配置模式下输入 nat (inside) 100（指定转换的内部地址）命令，并按回车键，如图 10-36 所示。



图 10-35　退出接口模式



图 10-36　指定内部转换地址

（15）在配置模式下输入 global (outside) 1 219.140.164.27-219.14.164.30 netmask 255.255.255.0（配置地址池）命令，并按回车键，如图 10-37 所示。

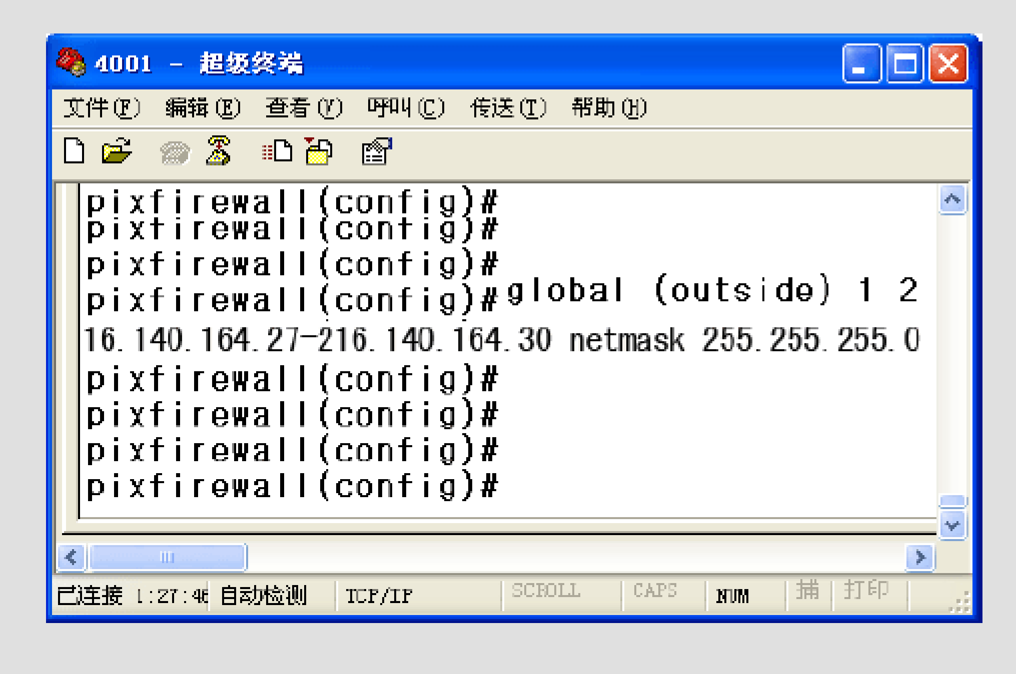


图 10-37　配置地址池

第11章 入侵检测系统

随着个人、机构日益依赖于 Internet 进行通信、协作及销售，对安全解决方案的需求急剧增长。据统计，全球 80%以上的入侵来自于内部。由于性能的限制，防火墙通常不能提供实时的入侵检测能力，对于企业内部人员所做的攻击，防火墙形同虚设。

入侵检测系统针对防火墙做了有益的补充，能够在入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击；在入侵攻击过程中，能减少入侵攻击所造成的损失；在被入侵攻击后，收集入侵攻击的相关信息，作为防范系统的知识，添加到知识库内，增强系统的防范能力，避免系统再次受到入侵。所以，也被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监听，从而提供对内部攻击、外部攻击和误操作的实时保护，大大提高网络的安全性。

本章对入侵检测系统的概念、系统分类、应用时的检测方式及发展方向进行阐述，以便网络用户方便快捷的使用。

本章学习要点：

- 了解 IDS 基本概念和系统分类掌握 IDS 的检测方式
- 熟悉 IDS 的应用
- 了解 IDS 的发展方向

11.1 IDS 的概述

入侵检测系统（Intrusion Detection Systems，IDS），是按照一定的安全策略对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或攻击结果，以保证网络系统资源的机密性、完整性和可用性。

11.1.1 IDS 的基本概念

在信息技术广泛应用于各个行业的同时，信息安全也便成为目前迫切需要解决的问题。从传统的信息安全来看，采用严格的访问控制和数据加密策略来防护，虽然在一定时间内取得了明显的效果，但在复杂系统中，采用这些策略明显是不充分的。确切来讲，它们是系统安全不可缺的部分，但不能完全保证系统的安全。

在信息安全的发展历程中，实现对入侵行为的检测技术渐渐被人们重视，且网络管理专家们要求有一种设备，能够通过从计算机网络的若干个重要位置收集信息并进行分析，从中

发现网络中是否有违反安全策略的行为和被攻击的迹象，这种设备就是现在人们普遍使用的入侵检测系统。

它可以说是防火墙系统的合理补充和延伸。如果说防火墙是第一道安全闸门，入侵检测系统则可以说是第二道安全闸门，能够在不影响网络性能的前提下，实时、动态地保护来自内部和外部的各种攻击，同时有效地弥补防火墙所能达到的防护极限。

通常入侵检测系统为了分析、判断特定行为或者事件是否为违反安全策略的异常行为或者攻击行为，需要经过信息收集、信息分析、事件报警/响应 3 个阶段，如图 11-1 所示。

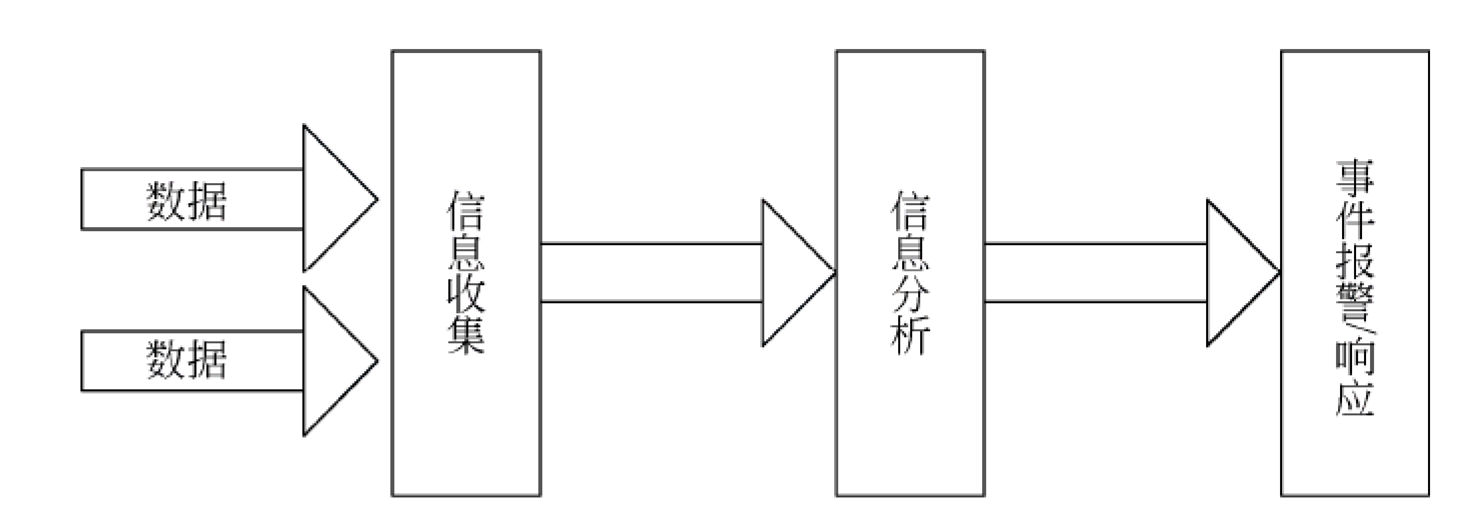


图 11-1　入侵检测系统工作流程图

1. 信息收集

信息收集包括收集系统、网络、数据及用户活动的状态和行为。而且，需要在计算机网络中的不同位置（不同网段和不同计算机）收集信息，这除了尽可能扩大检测范围的因素外，还可以对来自不同源的信息进行特征分析比较，得出问题所在的因素。

另外，入侵检测很大程度上依赖于收集信息的可靠性和正确性，所以，很有必要只利用所知道的真正的和精确的软件来报告这些信息。由于黑客经常替换软件以移走这些信息，例如，替换被程序调用的子程序、记录文件和其他工具；对系统的修改可能使系统功能失常但仍和正常的一样，例如，UNIX 系统的 PS（查看系统进程）指令可以被替换为一个不显示入侵过程的指令，或者是编辑器被替换成一个读取不同于指定文件的文件（黑客隐藏了初始文件并用另一版本代替）。因此，这就需要保证用来检测网络系统的软件的完整性，特别是入侵检测系统软件本身应具有相当强的坚固性，从而防止被篡改而收集到错误的信息。入侵检测利用的信息一般来自以下 3 个方面（这里不包括物理形式的入侵信息）。

❑ **系统和网络日志文件**

黑客经常在系统日志文件中留下他们的踪迹，因此可充分利用系统和网络日志文件信息。日志中包含发生在系统和网络上的不寻常活动的证据，这些证据可证明有人正在入侵或已成功入侵系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。另外，日志文件中还记录了各种行为类型，每种类型又包含不同的信息，例如，记录“用户活动类型”的日志就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。很显然地，对用户活动来讲，不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等。

❑ **非正常的目录和文件**

网络环境中的文件系统包含很多软件和数据文件，它们经常是黑客修改或破坏的目标。

目录和文件中非正常改变（如修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。通常黑客会替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

❑ **执行非正常的程序**

网络系统上执行的程序，一般包括操作系统、网络服务、用户启动的程序和特定目的的应用，如 Web 服务器。一般，每个在系统上执行的程序由一到多个进程来实现，一个进程的执行行为由它运行时执行的操作来表现，操作执行的方式不同，它利用的系统资源也就不同。操作包括计算、文件传输、设备和其他进程，以及与网络中其他进程的通信。

一个进程出现了不期望的行为，可能表明黑客正在入侵系统，并且会将程序或服务的运行分解，从而导致失败，或者是以非用户或管理员意图的方式操作。

2. 信息分析

对收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般可通过模式匹配、统计分析和完整性分析 3 种技术手段进行分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

❑ **模式匹配**

模式匹配就是将收集到的信息，与已知的网络入侵和系统已有模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单（如通过字符串匹配以寻找一个简单的条目或指令），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）。

一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断地升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的新黑客攻击手段。

❑ **统计分析**

统计分析方式首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。其比较过程与模式匹配有些相似，测量属性的平均值将被用来与网络、系统的行为进行比较，任何在正常值范围之外的观察值，就认为有入侵发生。例如，本应该使用默认 GUEST（来宾）账号登录的，却用 ADMINI（管理员）账号登录。

该分析方式的优点是可检测到未知的入侵和较为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法，但目前正处于研究热点和迅速发展之中。

❑ **完整性分析**

完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的、被特洛伊化的应用程序方面特别有效。完整性分析利用强有力的加密机制，称为消息摘要函数（例如 MD5），能够识别微小的变化。

其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要因为成功的攻击导致了

文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，用于事后分析而不用于实时响应。尽管如此，完整性检测方法还应该是网络安全产品的必要手段之一。例如，可以在每一天的某个特定时间内开启完整性分析模块，对网络系统进行全面的扫描检查。

3. 事件报警/响应

当 IDS 一旦检测到了攻击行为，IDS 的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应，通常都包括通知管理员、记录在数据库。

11.1.2 IDS 基本组成

IDS 进行信息收集、分析及事件报警/响应时，主要由对网络数据进行监听的网络传感器（Sensor）；通知管理员这些数据包的警报系统；显示这些警报的命令控制板；在可能的入侵发生时可以自动采取对策的响应系统；IDS 用于标识通信的功能攻击签名或者行为的数据库，并借此采取对策这些组件来完成，同时它们都是 IDS 基本组成部分。

1. 网络传感器

网络传感器就好像是入侵检测系统的“眼睛”。类似连接到门上的开关，或者是一个粘在玻璃窗上的金属条，当门被打开或者玻璃破裂时，就会发出警报（除非禁用或者关闭了该系统）。

由于性能和安全等方面的需求，现在的传感器多采用专用的设备来实现，它的一块网卡通过混杂模式连接在被检测的网段上负责收集网络数据包；另一块网卡用于管理，其他模块负责分析和处理数据包。

另外，入侵检测很大程度上依赖于收集信息的可靠性和正确性，所以用于信息收集的传感器需要在网络系统中的若干不同网段关键位置进行收集，如图 11-2 所示。然后，再根据 IDS 收集的信息进一步分析并作出反应。

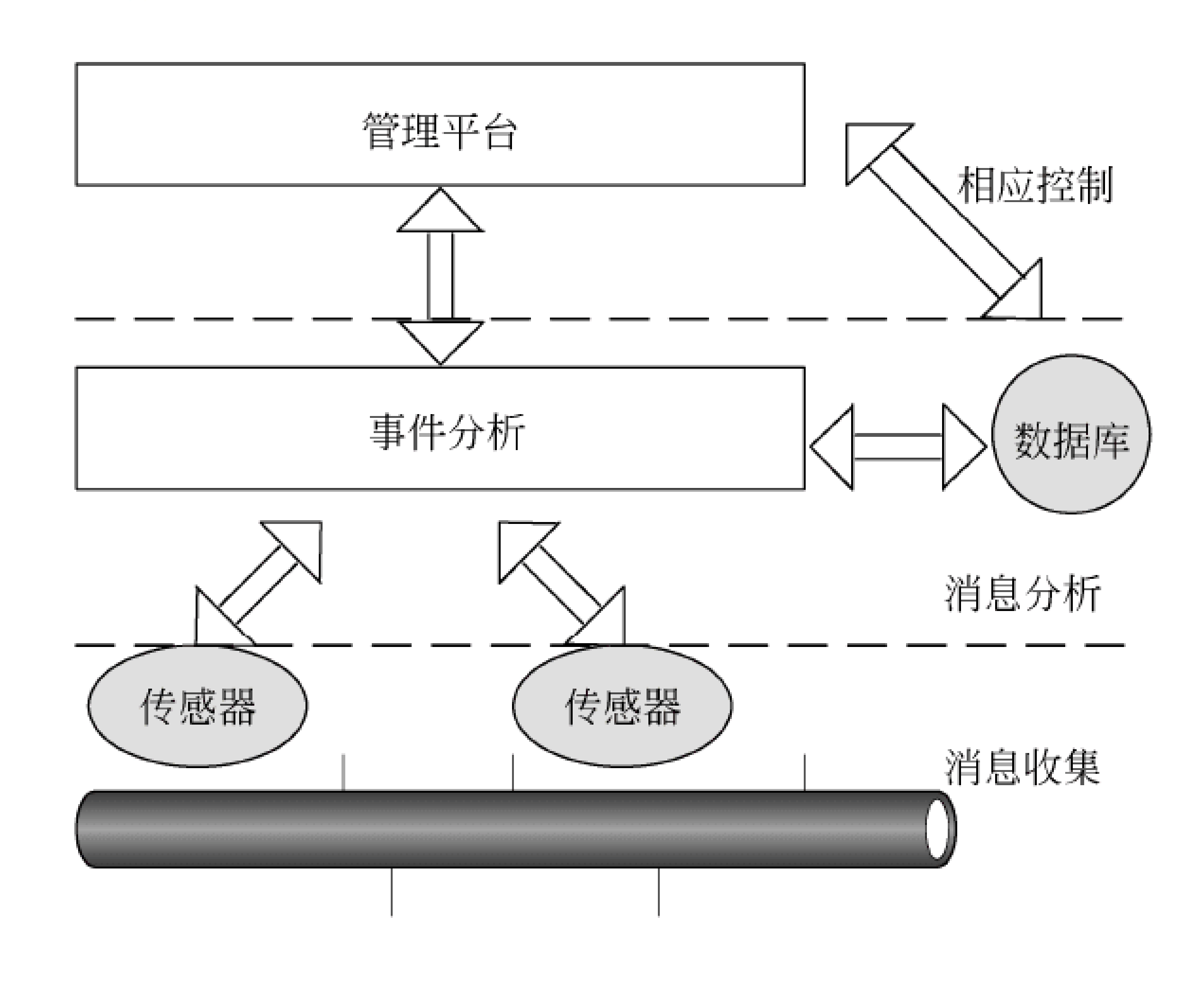


图 11-2　IDS 基本结构示意图

2. 报警系统

当特定类型的事件发生时，如窗户破裂或者门被打开，家庭的防盗警报器系统就会发出警报声音。IDS 的工作方式非常相似，当它遇到可疑的数据包或者通信模式时，就会发出声音或者发送警报。响应这样的事件时，IDS 使用的是触发器，可以使警报发出的一组情形。警报消息可以采取很多形式，如弹出式窗口、电子邮件消息、声音或者发送到寻呼机的消息。

可以引发警报的触发器有两种类型：异常检测和滥用检测。下面将分别讨论这两种触发器。

❑ **异常检测**

当系统检测到的事件与已定义为“正常”的行为不一致时，它就会发出警报。这有时被称为基于配置文件的检测，因为它将当前的网络通信与正常网络用法的配置文件相比较。如果特别关心来自机构内部的网络滥用情况，或者想监视所有出入电子邮件、Web 和 FTP 服务器的通信，就可以使用异常检测。

异常检测系统要求以上系统的每个授权用户或组织都使用配置文件。这些配置文件是特性的集合，描述用户通常在网络上访问的服务器和资源。有些 IDS 系统具有在“训练期间”，即 IDS 在此期间监视网络通信，观察什么构成了“正常”的网络行为。自己创建用户配置文件的能力。否则，就需要用户亲自创建配置文件。由于大型公司网络可能由分成多个组的几百个甚至几千个用户组成，因此配置文件的配置是一个相当费时的工作。

IDS 使用的配置文件的准确性对于它检测来自这些配置文件的异常情况的有效性有着直接的影响。如果配置文件准确的话，IDS 将只对真正的攻击发出警报。如果配置不完整或者不准确，那么将发送结果是假阳性的警报：由合法网络通信而非真正攻击生成的警报。它们还会在公司的员工中间引起不必要的惊慌，如果这样的警报发生得太频繁，员工可能就不再认真地对待它们。用户配置的基于异常的 IDS 需要具有足够准确的配置文件，使假阳性警报减至最低限度，甚至将它们完全消除。另外，还需要足够准确的 IDS，以免出现假阴性警报：真正的攻击已经发生，但是由于没有针对它们的配置文件，以至于 IDS 检测不到它们。

❑ **滥用检测**

滥用检测在响应滥用时发出警报的 IDS 将使用签名，签名是匹配已知攻击示例的特性的集合。如果有时间和能力（或许还需要有软件）了解由这样的系统生成的大量日志文件，就可以选择滥用检测。如果机构想使用基本的 IDS，并且主要关心的是试图从 Internet 上访问主机的黑客发起的已知攻击，那么就应当选择基于滥用的系统，并定期更新系统的签名。

基于异常的检测触发警报时，其根据是与公司内部用户或者组织的“正常”网络行为不相一致的情况，而滥用检测是基于来自公司外部的已知攻击的特性签名触发警报。配置 IDS 的网络工程师要研究众所周知的攻击，并记录与每个签名有关的规则。然后把这样签名的数据库用于 IDS。由于 IDS 配图有一组签名，因此在安装之后，它就可以立即开始保护网络。这与基于异常的 IDS 不同，在它开始保护网络之前，必须对它进行训练，使它认识“正常”的网络通信。

3. 命令控制台

命令控制台是一种软件，它向管理员提供到 IDS 的图形前端接口。该控制台使管理员可

以接收和分析警报消息，以及管理日志文件。在部署了一个以上 IDS 的大型网络中，单个控制台可以让管理员跟上大量的事件，以便快速响应并采取对策。

如 Symantec Man Hunt（www.symantec.com）或者 Cisco IDS Host Sensor 这样的程序可以提供单个接口，以查看当前发生的安全事件，或者查看最近发生的警报或入侵企图，以便在比较时使用。

用户可以按照和防火墙差不多的方法设置 IDS 的安全策略。IDS 可以从整个网络中与命令控制台相连的安全设备收集信息，在命令控制台可以检查和评估这些安全设备。为了使响应速度最快，通常将命令控制台安装在专用于 IDS 的计算机上。由于在检测可疑的事件时，命令控制台设备的宿主计算机忙于备份文件或者执行防火墙功能，所以它应当快速进行响应。

4. 响应系统

当检测到入侵时，有些比较高级的 IDS 可以设置成采取一些对策，如复位所有的网络连接。当检测到攻击时，不应当将此代替网络管理员采取适当的对策。管理员可以用自己的判断来确定警报是由假阳性攻击还是真正的攻击（有时被称为真阳性攻击）触发的。如果攻击是真的，管理员的判断还可用于估计攻击的严重性，并确定是否应当升级（升级即提高到更高的级别）响应。

5. 攻击签名或行为的数据库

网络管理员在评估安全警报时才可以运用判断能力，而入侵检测系统没有判断力。因为它们需要信息源，然后凭此来比较它们监视的通信。基于滥用的系统要求有已知攻击签名的数据库；如果传感器检测到的一个数据包或者一系列数据包与其中的一个签名相匹配，它就会发出警报。

攻击签名数据库的关键在于它们一直保持最新状态；如果新型的攻击没有添加到系统的可用签名中，这种攻击很快就可以击败 IDS。IDS 供应商应当为用户提供一种方法，使用户可以下载新的条目，从而将它们添加到数据库中。而只依赖于签名的系统的问题在于它们是被动的；它们监视通信，将通信与数据库进行比较，每当数据包匹配可用的签名时就发出警报，但是这将产生大量的假阳性警报。大多数 IDS 都允许管理员将他们自己的自定义规则添加到数据库中，以减少“假警报”的数量，承认克服这样的被动性。

IDS 的异常检测方法也使用存储信息的数据库，以此来比较网络通信。例如，Securify 公司的 SecurVantage3.0 每过一段特定的时间就对认为是“正常”的网络通信进行扫描。因为 SecurVantage 开发了一组策略，描述谁通常可以使用网络设备，以及如何使用设备，并且出现任何与这组收集的策略不一致的情况都将触发警报。

11.1.3　IDS 提供的信息

入侵检测系统只能报告那些为它配置好的应报告的内容。IDS 配置中包含两个部分：第一部分是已经编译在系统中的攻击特征；第二部分是管理员发现的需要注意的任何例外事件。这可能包括某种类型的通信数据或某种类型的日志消息。

对于预先编译的特征，厂商或系统的开发人员加入了他们自己对这些事件重要性的理解。

对于特定机构而言，这些事件的重要性或许与制造商所指定的有很大不同。因此可能需要修改一些特征的默认优先级设置，或者关掉一些对机构不适用的特征。

假设 IDS 配置正确，那么 IDS 会显示侦察事件、攻击事件、策略违反事件、可疑事件及无法解释的事件这些信息。

1. 侦察事件

侦察事件是攻击者在实际攻击之前，收集有关系统信息的企图。这些事件可以分为 5 类。

❑ **盗窃性扫描**

盗窃性扫描是以保护源系统不被发现的方式，找出网络中现有系统的企图。在基于网络的 IDS 检测器上，这种类型的扫描可能显示为 IP 半扫描或 IP 盗窃性扫描，它一般针对的是大量 IP 地址。对这种扫描的响应是找出源并通知源系统（很可能是被攻击的系统）的所有者。

❑ **端口扫描**

端口扫描用于找出网络上的系统所提供的服务。当一个系统上的几个端口在短时间内被打开时，HIDS 可以发现端口扫描。而基于网络的 IDS 检测器和一些基于混合式的 IDS 检测器，不仅可以发现端口扫描，而且还会将其作为端口扫描事件来报告。对这种扫描的响应与对盗窃性扫描的响应一样。

❑ **特洛伊木马扫描**

特洛伊木马有很多种。基于网络的 IDS 检测器具有可以识别多种特洛伊木马的特征。遗憾的是，到达特洛伊木马程序的通信数据，常常是通过数据包的目标端口来识别的。这样，会产生许多误报。对于特洛伊木马事件，应该检查通信数据的源端口。例如来自端口 80 的通信数据，很可能是来自一个 Web 站点的回复通信数据。

最常见的特洛伊木马扫描类型是 Back Orifice。Back Orifice 使用端口 31337，攻击者通常会在一个地址范围内扫描这个端口。Back Orifice 控制台还包括一项 ping 主机的功能，这个过程可以自动进行。除非发现来自一个内部系统的通信数据，否则不需要为此产生担心。同样，恰当的响应是与源系统的所有者进行联系，因为这个系统很可能受到了攻击。

❑ **薄弱点扫描**

在基于网络的 IDS 检测器上，薄弱扫描表现为大量的不同攻击特征。通常，这种扫描针对几个确实存在的系统。很少遇到针对一个不包含活动系统的地址范围进行的薄弱点扫描。

黑客进行的薄弱点扫描与由安全测试公司进行的薄弱点扫描无法区分开发（在许多情况下，他们使用的工具是相同的）。在这两种情况下，扫描本身不会对系统造成破坏，但是如果黑客进行了扫描，并且系统上存在进行攻击的薄弱点，那么黑客就会了解这些信息。应该与源系统的所有者联系，并对内部系统进行检查，以确保它们安装了最新的补丁程序。

❑ **文件侦听**

对文件授权进行侦听或测试一般由内部用户进行。用户试图找出哪些文件可以访问以及它们的内容是什么。这种类型的侦察只能在基于混合式的 IDS 检测器上显示，并且只有在系统记录未经授权的访问企图时才行。单一事件可能是无意的错误，但是如果反复出现，则应该与用户联系，看一看他正在做什么。

这些事件主要发生在网络上，而且大多数是从 Internet 向具有外部地址的系统实施的。侦察事件试图获得有关系统的信息，它们不能破坏系统。通常，一些商业 IDS 系统被配置为侦

察事件赋予很高的优先级。考虑到这些事件不会破坏系统，所以这种配置似乎是不恰当的。

2. 攻击事件

攻击事件是那些需要快速响应的事件。在理想情况下，如果已知内部薄弱点受到了攻击，则应该将 IDS 配置只找出具有较高优先级的事件。在这种情况下，应该立即实施应急响应过程。

要注意的是，IDS 无法知道实际攻击与看起来像攻击的薄弱点扫描有何区别。IDS 管理员必须评估 IDS 提供的信息，这样才能确定这是否是真正的攻击。要查看的第一件事情是事件的数量。如果在短时间内出现了对同一系统的不同攻击特征，那么这很可能是薄弱点扫描而不是真正的攻击。如果发现了针对一个或多个系统的同一种攻击特征，则可能是真正的攻击。

3. 策略违反事件

大多数 IDS 系统对于事件具有如下的特征。

- 文件共享（Gnutella、Kazaa 等）。
- 即时的信使。
- Telnet 会话。
- “r”命令（rlogin、rsh、rexec）。

在大多数机构中，这种通信方式的用户都会违反机构的策略。遗憾的是，这种策略违反的情况对于机构而言比受到攻击更危险。多数情况下，事件已经发生过。因此文件已经共享，或者系统被配置允许 rlogin。

用户的机构响应各种违反策略的情况取决于机构的内部策略和程序。但是至少系统管理员或相关人员应该被告知策略，便于他们理解机构的策略。

4. 可疑及无法解释的事件

不能明确地归类的事件称为可疑事件。可疑事件就是无法理解的事件。例如，Windows NT 服务上的注册键被修改，但是没有可解释的原因。它不像受到了攻击，也没有迹象表明它为什么会被修改。另一个例子是数据包的题头标识与协议标准不符合。这是侦察扫描企图？还是存在出现故障网卡的系统？或者是传输中出现了错误的数据包？由 IDS 提供的信息不能提供足够的信息来回答这些问题，并确定事件是无害的还是一次攻击。

同样可疑的是，在内部网络中发现没有预期的通信数据。如果桌面计算机开始向其他系统请求 SNMP 信息，那么这是一次攻击还是系统配置出现了错误？应该在资源许可的范围内对可疑事件进行调查。

11.2　IDS 系统分类

根据 IDS 检测对象和系统加载位置的不同，可将其分为基于主机的 IDS（HIDS）、基于网络的 IDS（NIDS）和混合式 IDS 3 种类型。HIDS 驻留于特定的主机上，寻找这台主机上受攻击的迹象。NIDS 在一个单独的系统上监视网络通信数据，寻找经过这部分网络的攻击迹象。

混合式 IDS 可同时放置在网络和各个主机上，提供更高的安全性。

11.2.1 基于主机的 IDS

基于主机的 IDS（HIDS）是一种检测器系统，它被加载到机构的各种服务器上，并受到中央管理器的控制。检测器可以查找各种事件，在特定的服务器上采取行动，或者发出通知信息。HIDS 检测器监视与所加载的服务器相关的事件。HIDS 检测器还可以判断一种攻击是否成功，因为攻击发生在检测器所在的平台上。

可以看到，不同类型的 HIDS 检测器可以完成不同类型的 IDS 目标。并不是所有的检测器都适用于各种类型的机构，甚至无法适用于同一机构内的所有服务器。因此必须对每一种服务器确认最合适的检测器，这是很重要的。还必须注意，HIDS 系统可能成本要高于基于网络的系统，因为每一种服务器都必须具有检测器许可（检测器单位价格较低，但是数量众多的检测器会导致整体成本较高）。

与 HIDS 系统相伴的另一个问题是服务器上的处理器容量。运行在服务器上的检测器进程会占用 CPU 容量的 5%～15%。如果检测器位于载荷较大的系统上，就会影响验证性能，需要购买更高级的系统。目前，有以下 5 种基本的 HIDS 检测器类型。

1. 日志分析器

日志分析器的功能是将 HIDS 收集并储存到日志文件内的信息，进行分析。当一个进程运行于服务器之上，相对于监视系统上正确的日志文件，如果一个日志条目显示与 HIDS 检测器进程中的某些标准匹配，就会发生某种动作。不过，大多数日志分析器配置来查找指示安全事件的日志条目。另外，系统管理员通常可以定义其他感兴趣的日志条目。

日志分析器本质上是响应系统。换句话说，在发生某种事件之后，它们会作出响应。因此其发出的通知表示系统已经受到了攻击。在大多数情况下，日志分析器无法阻止攻击成功入侵系统。

实际中，日志分析器适合于记录合法用户在内部网络上的活动。因此如果机构关注系统管理员或其他授权用户的活动，日志分析器就可以记录活动，并将这些活动记录发送到管理员或用户无法访问的系统。

2. 基于特征的检测器

这种检测器具有一组内置的安全事件特征，这些特征与输入的网络通信或者日志条目对照。基于特征的检测器和日志分析器的区别在于它增加了分析输入通信的功能。

基于特征的系统可以检测出针对系统的攻击，因此这些系统可以发出关于攻击的附加通知。但是，在 HIDS 检测器作出反应之前，攻击可能成功，也可能失败，使得检测器也具有响应的特性。基于特征的 HIDS 检测器也可以用于记录内部系统上的授权用户的活动。

3. 系统调用分析器

系统调用分析器可以分析应用程序和操作系统之间的调用，以确认安全事件。这种类型的 HIDS 检测器在应用程序和操作系统之间安装了软件。当应用程序希望执行动作时，针对操

作系统执行某种动作的调用就会得到分析，并与特征数据库比较。这些特征是各种行为的范例，这些行为指示攻击，或者表示 IDS 管理员感兴趣的事件。

系统调用分析器不同于日志分析器和基于特征的 HIDS 检测器，即它们可以阻止动作的发生。如果应用程序发出了调用匹配缓存溢出的特征，检测器就可以阻止这种动作，从而防止系统受到攻击。

4. 应用行为分析器

应用行为分析器类似于系统调用分析器，即它们都实现为应用程序和操作系统之间的程序段。在行为分析器中，检测器检查调用，确认是否允许应用程序执行动作，相反不会检查调用是否类似攻击。例如，通常允许 Web 服务器端口 80 上接受网络连接，在 Web 目录中读取文件，在端口 80 之间的连接上发送文件。如果 Web 服务器试图从其他位置写入文件，读取文件，或从其他位置打开新的网络连接，检测器会监视不正确的行为，并阻止动作的发生。

配置这些检测器时，必须创建每一种应用程序所允许的动作。这些产品的开发商具有适用于一般应用程序的模板。所有自行开发的应用程序必须检查，确认通常允许它们所发生的动作，并编程进入检测器中。

5. 文件完整性检查器

文件完整性检查器检查文件的变动。这可以通过使用密码学校验或者数字特征完成。如果初始文件的任何变动（包括创建时间和大小的属性的变化），则相应的特征就会改变。人们开发了用于这个进程的算法，使得很难做出文件修改，却留下了使用特征。

根据检测器初始配置情况，被检测变动情况的每一个文件都通过此算法运行，以创建初始特征。其数字被存储在安全的位置。每一个受监控的文件都定期重新计算特征，并与初始特征比较。如果匹配，则文件没有修改。如果不匹配，则文件已经被修改了。

文件完整性检查器不会给出攻击的任何指示，却详细描述攻击的结果。因此，如果 Web 服务器受到攻击，则攻击本身不会被检测到，但是网站的涂改或端点主页的修改却会被检测到。其他类型的系统攻击也是如此，因此许多这种攻击都包括对系统文件的修改。

11.2.2　基于网络的 IDS

基于网络的入侵检测系统（NIDS）放置在比较重要的网段内，不停地监视网段中的各种数据包，并对每一个数据包进行特征分析。如果数据包与系统内置的某些规则吻合，入侵检测系统就会发出警报甚至直接切断网络连接。目前，大部分入侵检测系统是基于网络的。

图 11-3 展示一个典型 NIDS，一个传感器被安装在防火墙外探查来自 Internet 的攻击。另一个传感器安装在网络内部探查那些已穿透防火墙的入侵和内部网络入侵和威胁。

基于网络的入侵检测系统，通常利用一个运行在随机模式下的网络适配器来实时监视并分析通过网络的所有通信业务。它的攻击辨识模块通常使用标志模式、表达式或字节匹配、频率或穿越阈值、低级事件的相关性这 4 种常用技术来识别攻击。

一旦检测到了攻击行为，IDS 的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应。反应因系统而异，但通常都包括通知管理员、中断连接并且/或为法庭分析和证据收

集而做的会话记录。

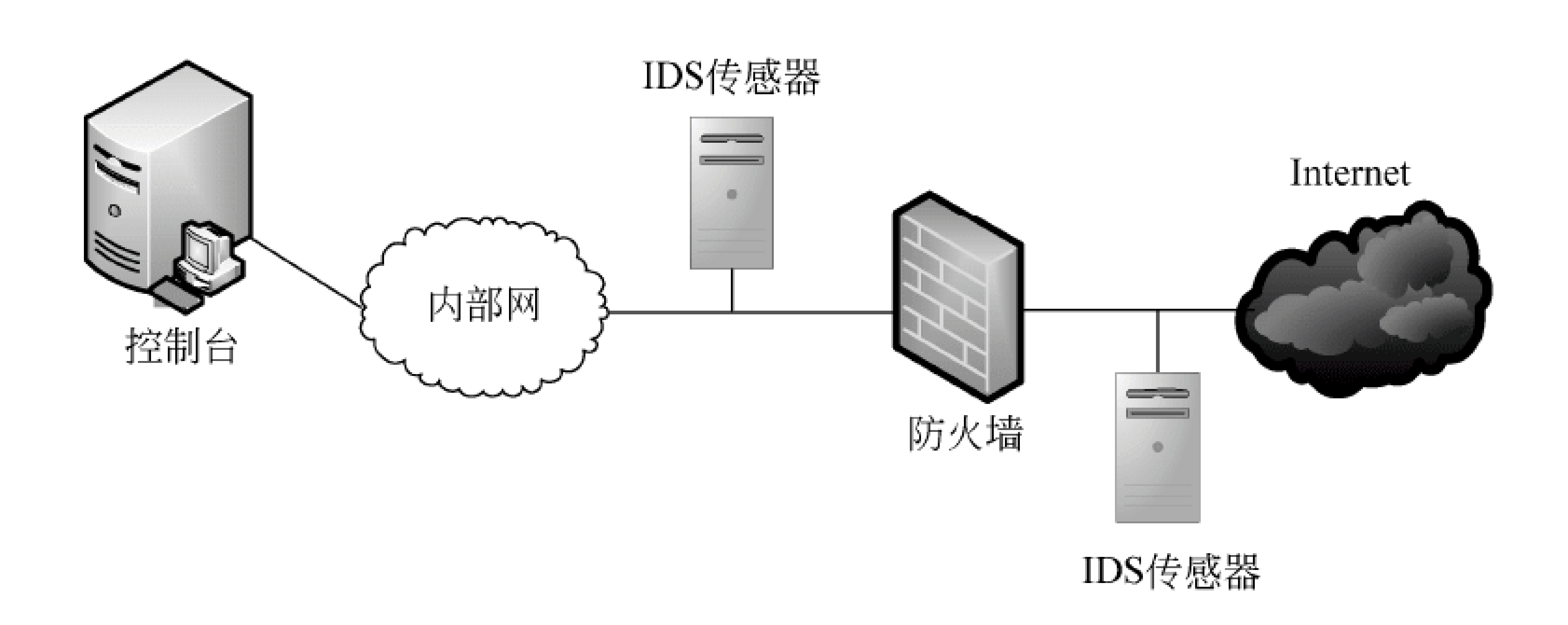


图 11-3　基于网络的检查系统

1. 优点

基于网络的 IDS 之所以成为安全策略的实施中的重要组件，因为它具有以下仅靠基于主机的入侵检测法无法提供的优点。

❑ **检测基于主机的系统漏掉的攻击**

基于网络的 IDS 检查所有包的头部从而发现恶意的和可疑的行动迹象。基于主机的 IDS 无法查看包的头部，所以它无法检测到这一类型的攻击。例如，许多来自于 IP 地址的拒绝服务型和碎片型攻击只有在它们经过网络时，才可以在基于网络的 IDS 中通过实时监测包流而被发现。

基于网络的 IDS 可以检查有效负载的内容，查找用于特定攻击的指令或语法。例如，通过检查数据包有效负载可以查到黑客软件，而使正在寻找系统漏洞的攻击者毫无察觉。由于基于主机的系统不检查有效负载，所以不能辨认有效负载中所包含的攻击信息。

❑ **攻击者不易转移证据**

基于网络的 IDS 使用正在发生的网络通信进行实时攻击的检测，所以攻击者无法转移证据。被捕获的数据不仅包括攻击的方法，而且还包括可识别的入侵者身份及对其进行起诉的信息。

❑ **实时检测和响应**

基于网络的 IDS 可以在恶意及可疑攻击发生的同时将其检测出来，并作出更快的通知和响应。例如，一个基于 TCP 协议对网络进行拒绝服务的攻击，可以通过基于网络的 IDS 发出 TCP 复位信号，在该攻击对目标计算机造成破坏前，将其中断。而基于主机的系统，只有在可疑的登录信息被记录下来以后，才能识别攻击并作出反应，不过此时关键系统可能早就遭到了破坏，或是运行基于主机的 IDS 的系统已被摧毁。另外，实时 IDS 还可根据预定义的参数作出快速反应，这些反应包括将攻击设为监视模式以收集信息，立即中止攻击等。

❑ **检测未成功的攻击和不良意图**

基于网络的 IDS 增加了许多有价值的数据，以判别不良意图。即便防火墙正在拒绝这些尝试，但位于防火墙之外基于网络的 IDS 可以查出躲在防火墙后的攻击意图。基于主机的系统无法查到从未攻击到防火墙内主机的未遂攻击，而这些丢失的信息对于评估和优化安全策略是至关重要的。

❑ **操作系统无关性**

基于网络的 IDS 作为安全监测资源，与主机的操作系统无关。与之相比，基于主机的系统必须在特定的、没有遭到破坏的操作系统中才能正常工作，生成有用的结果。

2. 缺点

网络入侵检测系统有如下弱点。

❑ **无法跨网段检测**

网络入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中就会出现监测范围的局限，而安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。

❑ **不易检测复杂攻击**

为了提高网络入侵检测系统性能，通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。另外，网络入侵检测系统处理加密的会话过程较困难，目前通过加密通道的攻击并不多，但随着 IPv6 的普及，这个问题会越来越突出。

11.2.3　混合式入侵检测系统

混合式入侵检测系统可将一个以上系统的功能组合在一起，以便获得更强的灵活性和安全性。混合式 IDS 的目的，在于获得比单一基于主机或者基于网络的实现方式更高的安全性和更大的灵活性，因为这些基于主机的 IDS 和基于网络的 IDS 各有优缺点。下面将介绍各种混合式 IDS 的实现方式——组合 IDS 传感器位置、组合 IDS 检测方法、补偿 IDS 和分布式 IDS。

1. 组合 IDS 传感器位置

IDS 混合实现方式的一种类型，是将基于主机的系统与基于网络的系统组合起来。这种组合使传感器可同时放置在网络和各个主机上，这样网络就能报告针对特定网段或者整个网络的攻击。

另一方面，基于主机的 IDS 可以保护包含特别敏感信息（如工作记录或者收入支出记录的数据库）的各台计算机。在计算机（特别执行分布式基于主机 IDS 的计算机）上安装了 IDS 后，就可以实时地分析数据，并且可以发出警报，通知管理员在可以立即确认的关键资源处存在可能的未授权访问企图。

2. 组合 IDS 检测方法

IDS 混合实现方式的另一种类型是组合异常检测和滥用检测。该组合有助于克服每种检测的局限性，将已知攻击签名的数据库设置好以后，系统就可以立即运行，并且可以有效地抵御外部攻击；将基于异常的系统设置好以后，就可以使警报系统保持灵活性，并且能够检测与正常的使用模式不一致的内部滥用。

组合了异常检测和滥用检测方法的混合式 IDS 可以响应最新的、以前未报告过的攻击。它还具有响应来自内部和外部源的攻击。

其缺点是管理员需要处理更多的配置和协调工作。从多处来源收集的数据必须归集于一处，在此位置便于迅速检查和分析数据。

3. 补偿 IDS

补偿 IDS 是一种基于网络的 IDS，因为它使用的传感器分布在网络中，并且要从这些传感器收集数据，然后发送到集中式命令控制台。但是，传感器安装在选定的主机以及网段上。与基于主机的 IDS 不同，不必将传感器安装在网络中的每个主机上。只需将它们安装在需要特殊保护的主机上，如保存一个公司的专用产品信息的数据库。

4. 分布式 IDS

分布式入侵检测系统增强了快速响应，其中将多个入侵检测设备部署在网络上监视通信和报告可疑事件。通过使用多个 IDS 而非单个 IDS，开发了使管理员可以将无害的异常事件和真正的攻击区别开发的模式。MyNetWatchman（www.mynetwatchman.com）和 DShield（www.dshield.org）是两种著名的 IDS。DShield 的 Web 站点用来跟踪来自全球的攻击，并收集 Internet 用户自愿提交的数据。收集的数据越多，开发的模式越准确。DShield 将通知用户在提交日志文件中是否包含入侵模式，以便可以根据情况配置阻止入侵者的软件。

5. 混合式 IDS 的优缺点

由于能够将基于网络的配置和基于主机的配置的各个方面组合，所以混合入侵检测系统具有巨大的优势。用户可以利用基于网络的传感器监视整个网络，并且可以利用基于主机的传感器监视到在各台计算机的攻击。混合式布局的缺点在于需要使不同的系统协调工作。此外，从多个系统收集的数据可能也难以被轻松地理解和分析。

11.2.4 IDS 相关软件

目前网络中，存在许多种与 IDS 相关的软件，它们有的可以免费获得，有些商业程序则需要购买。其中，最常见的 IDS 相关软件有 Snort、Norton Internet Security、Tripwire 和 Cisco Secure IDS 等。

1. Snort

Snort 是由 Martin Roesch 和 Brain Caswell 制作的 IDS 免费软件，它是一个小型的程序，使用的系统资源较少，适合于监视小型网络或者单个主机上的通信。可以将 Snort 安装在位于网络周边的计算机上。它还可以应用于家庭或者小型商业网络上的专用计算机上。

Snort 具有一个规则文件集合，这些文件是为各种类型的网络通信定制的，在总体配置文件 snort.conf 中可以激活它们。独立的规则将应用于端口扫描、后门攻击、Web 攻击和许多其他类型的潜在入侵。规则文件是基于文本的；要在文本编辑器中打开规则文件，然后对它们进行检查和编辑，使其适合用户自己的网络。

snort.conf 配置文件易于编辑，并且可以对它进行定制，以适合其他大量的事件。此外，其他配置文件包含的变量使用户可以保护网络上的 SMTP、HTTP 和 SQL 服务器，否则的话，

由于通过这些服务器的通信量很大，它们就有可能引起假警报。另外还提供了各种各样用于 Snort 的 GUI 接口。这些 GUI 包括 IDS Center 或者 SnortSnarf。

2. Norton Internet Security

Symantec 公司 Norton Internet Security 是一种个人防火墙程序，用于保护基于家庭独立计算机或者小型网络上的计算机。但是，这种程序还包含一些入侵检测功能。这些功能专门用于阻止端口扫描，以及由众所周知的特洛伊木马程序使用的端口上的攻击企图。如果检测到攻击，那么称为 AutoBlock 的功能将使黑客与用户的计算机之间的通信停止 30 秒。在这 30 秒的时间内，黑客可能会转向另一台计算机去尝试攻击。如果黑客试图对用户的计算机进行同样的攻击，通信将被再次终止。

和其他个人防火墙程序一样，Norton Internet Security 具有“学习”什么构成“正常”的网络使用、什么与这样的使用相背离的能力。它允许用户建立规则，阻止与正常使用不一致的通信。当遇到的通信可能是入侵时，将出现弹出式警报消息。但是，该程序缺乏设置用户配置文件的能力，并且除了前面提到的端口扫描和特洛伊木马攻击之外，它没有使用一组攻击签名。

3. Tripwire

Tripwire 最初是 1992 年在 Purdue 大学开发的，长期以来，一直是最受欢迎的软件 IDS 程序包之一。该程序的最新版本是 Tripwire 公司提供的 Tripwire for Network Devices，它使用基于异常的入侵检测。它首先建立正常网络使用的基准。在基准建立之后，在配置中出现的任何变化，例如在系统上创建新的文件，或者某个用户第一次访问服务器，都将触发警报消息。

该软件适合于需要密切监视员工活动的情况。Tripwire 维护着一个日志文件，它详细地记录每个用户和网络资源发生的每个交互作用。此外，自最后的“良好”配置建立以来，任何已经放置在网络资源上的新文件都将被记录，这使管理员可以迅速检测病毒或者蠕虫是否已经激活。

4. RealSecure

Internet Security Systems 公司提供的 RealSecure 是最全面、在市场上使用最广泛的产品之一。RealSecure 使用分布式客户-服务器体系结构。利用一个或者更多的 RealSecure 网络传感器产品，它可以扫描网络上的通信。此外，OS 和服务器传感器还可以监视出入主机的通信，以便检测所有未经授权的活动。这些可用的传感器彼此协作，使 RealSecure 可以起到混合式 IDS 的作用。

RealSecure 还包括一个称为 Workgroup Manager 的命令控制台，它可以提供到已安装的传感器的安全通信信道。该控制台使网络管理员可以使用具有 2000 多种已知攻击签名的数据库，执行警报监视。

5. Cisco Secure IDS

Cisco Secure IDS 利用攻击签名数据库检测入侵企图。这种基于网络的 IDS 使用传感器（具有自己的处理器、内存和网络接口卡的硬件设备）被放置在网络的周围，用于监视通信。警

报将发送到两个命令控制台之一：Cisco Secure Policy Manager 或者用于 UNIX 的 Cisco Secure IDS Director。

签名是 Cisco Secure IDS Director 的基础，可以供该系统使用的签名被分成各种类型的网络通信包括 IP 签名、ICMP 签名、TCP 签名、Web/HTTP 签名、匹配字符串的签名等。但是，该系统不仅仅将通信与其签名数据库进行比较，它监视网络通信时还要注意攻击的模式。除了监视通信外，还可以为传感器配置相应的规则，阻止所有来自不可靠 IP 地址的通信。

11.2.5　网管心得——网络入侵检测系统的主动响应技术

入侵检测系统（IDS）自 20 世纪 80 年代以来得到了极大的发展，典型的入侵检测系统通常采用静态异常模型和规则的滥用模型来检测入侵，这些 IDS 的检测基本是基于服务器或网络的，即主机 IDS 和网络 IDS。基于服务器的 IDS 采用服务器操作系统的检测顺序作为主要输入源来检测入侵行为，而基于网络的 IDS 则以监控网络故障作为检测机制，网络入侵检测系统是监视计算机网络系统中违背系统安全策略行为的过程。按照最为规范的形式来划分，入侵检测分为以下三个模块。

- **数据源**　提供用于系统监视的审计记录流。
- **分析引擎**　用于对审计数据进行分析，发现入侵或异常行为。
- **响应**　根据分析引擎的输出结果，产生适当的反应。

这些模块是相辅相成的，数据源为分析引擎提供原始数据进行入侵分析，分析引擎执行实际的入侵或异常行为检测，分析引擎的结果提交给响应模块，帮助采取必要和适当的动作，阻止进一步的入侵行为或恢复受损害的系统。同时响应模块作用的对象也包括数据源和分析引擎，对数据源来说，可以要求提供更为详细的信息，调整监视策略，收集其他类型的数据；对于分析引擎，则可以增加、删除或更改系统的检测规则，修正检测过程中的参考模型，调整系统的运行参数等。随着入侵检测技术的不断发展和完善，响应模块成为其中的关键部分，并得到了充分发展。

入侵检测系统中，在完成系统安全状况分析并确定系统所出问题后，则需要让人们知道这些问题的存在（在特定情况下，还要采取行动），这在入侵检测处理过程模型中称为响应。响应包括被动响应和主动响应。被动响应就是系统仅仅简单地记录和报告所检测出的问题，而主动响应则是系统要为阻塞或影响攻击进程而采取行动。在早期的入侵检测系统中被动响应是唯一的响应模式，随着技术的不断发展和人们对安全性要求的不断提高，主动响应成为现今入侵检测系统的主要响应模式。

在网络站点安全处理措施中，入侵检测的一个关键部分就是确定使用哪一种入侵检测响应方式以及根据响应结果来决定采取哪些行动，主动响应是主要方式。主动响应技术主要包括以下几种选项可供选择。

1. 入侵追踪技术

对入侵采取反击行动的方式，在一些组织和机构应用非常广泛，因为这些组织和机构的网络安全管理人员特别希望能够追踪入侵者的攻击来源，并采取行动切断入侵者计算机和网络的连接。但这一方式本身就存在安全漏洞，首先入侵者的常用攻击方法是使一个系统崩溃，

然后再利用它作为攻击另外系统的平台；其次，即使入侵者来自一合法控制的系统，但他也会利用 IP 地址欺骗技术使反击危害到其他人；并且反击的结果可能引起更猛烈的攻击，因为入侵者会从常规监视和扫描演变为全面攻击，从而使系统资源陷入危机；进一步讲，由于反击行动涉及重要法规和现实问题，所以这种响应方式也不应该成为最常用的主动响应。

2. 入侵警告和预防

对付入侵者也可以采取比较温和的方式。一方面，入侵检测系统可以有意地断开与其他网络的对话，例如向入侵者的计算机发送 TCP 的 RESET 包，或发送 TCMP Destination Unreachable（目标不可达）包，系统也可利用防火墙和网关阻止来自入侵的 IP 地址的数据包；另一方面，系统可以发邮件给怀疑入侵者的系统管理员请求协助以识别问题和处理问题。这种响应方式只能发现问题，处理问题，但对入侵检测系统的完善所起的作用并不明显，但在一些研究结构和院校得到一定应用。

这种响应方式是大部分商业入侵检测系统追求的，但由于应用起来涉及的问题比较多，发展相对比较慢。

3. 修正系统环境

修正系统环境类似于自动控制的反馈环节，并具有自学习进化功能。修正系统环境以修补导致入侵发生的漏洞为关键，通过增加敏感水平来改变分析引擎的操作特征，或通过插入规则改变专家系统来提高对一些攻击的怀疑或增加监视范围以比通常更好的采样间隔来收集信息。

这种响应方式由于相对于上一种响应来说相比更为缓和，若与提供调查支持的响应相结合可称为最佳响应配置，可广泛应用。

4. 收集额外信息

当被保护的系统非常重要且系统管理员需不断地进行法则矫正时，就需要收集入侵者的信息，并不断地改进和优化系统；并且可以将入侵转移到专用服务器。这些专用服务器设置被称为欺骗网技术，欺骗网技术就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，并且有一些可攻击窃取的资源（伪造或不重要的），并将入侵者引向这些错误的资源。它能够显著地增加入侵者的行为，在入侵者之前修补系统可能存在的安全漏洞。

从原理上讲，每个有价值的网络系统都存在安全弱点，而且这些弱点都可能被入侵者所利用。网络欺骗主要包括影响入侵者使之按照你的意志进行选择、迅速地检测到入侵者的进攻并获知其进攻技术和意图、消耗入侵者的资源 3 个作用。

以上 4 种响应模式是主动响应的主要表现形式，由于科研院所和商业公司所追求的目标和作用不同，响应模式的应用也是互不相同，因此主动响应技术的发展出现了多元化的发展趋势。

11.3　IDS 的检测方式

对各种事件进行分析，从中发现违反安全策略的行为是入侵检测系统的核心功能。从技

术上，入侵检测大体分为3类，分别为基于异常行为的检测技术（anomaly-based）、基于知识特征的检测技术（signature-based）和协议分析检测技术。

11.3.1　基于行为的检测

通过将过去观察到的正常行为与受到攻击时的行为加以比较，根据使用者的异常行为或资源的异常使用状况来判断是否发生入侵活动，其原则是任何与已知行为模型不符合的行为都认为是入侵行为。

异常检测的假设是入侵者活动异于正常主体的活动。这种活动存在 4 种可能：入侵性且非异常、非入侵性且异常、非入侵性且非异常、入侵且异常。如果能够建立系统正常行为的轨迹，那么理论上可以把所有与正常轨迹不同的系统状态视为可疑企图。根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。

异常检测的优点是可以发现未知的入侵行为，同时有一定的学习能力。异常检测的难题在于如何建立“活动简档”以及如何设计统计算法，从而不把正常的操作作为“入侵”（误报）或忽略真正的“入侵”行为（漏报）。对于异常阈值与特征的选择，是异常发现技术的关键。比如，通过流量统计分析将异常时间的异常网络流量视为可疑。

异常发现技术的局限是并非所有的入侵都表现为异常，而且系统的轨迹难于计算和更新。例如，当用户合法地改变行为模式时（如使用新的应用程序）系统会误报；入侵者可通过对正常行为模式缓慢地偏离使系统逐渐适应，导致系统漏报；对于新用户，系统的学习阶段何时结束不易确定，同时在该阶段难以对用户进行正常的检测。

另外，大多 IDS 是基于单包检查的，协议分析得不够，因此无法识别伪装或变形的网络攻击，也造成大量漏报和误报。

11.3.2　基于知识的检测

基于知识的检测方式是指在网络通信中搜索一系列字节或数据包队列以查找已知的恶意程序，也称为签名检测。该检测方式的最大好处是，如果清楚想要找出的网络行为，这种签名就很容易开发和理解。例如，能够利用一个签名寻找一个可利用的安全漏洞中的特定字符串来检测，并使用特定的缓存溢出安全漏洞实施攻击的企图。这个由基于知识的入侵检测系统产生的事件能够传达什么导致了报警，模式匹配在现代系统上能够很快完成，因此对于确定的一套规则来讲，进行这种检测所需要的计算能力是最小的。例如，如果要保护的系统仅通过 DNS、ICMP 和 SMTP 通信，所有的其他签名都将被删除。

签名引擎也存在着弱点。由于签名引擎检测已知的攻击，必须为每一种攻击制作一个签名，而且新的攻击还无法检测；签名检测通常是根据正常的表达和字符串设计的，因此签名引擎也会出现不正确的检测结果，且这种机制只是在线路上传输的数据包中检测字符串。

虽然签名对于检测以固定方式实施的攻击很成功，但是对于人工制作的或者具有自我修正行为功能的蠕虫发起的多种形式的攻击的检测就有些力不从心。有些利用安全漏洞允许恶意用户把攻击隐藏在“nop 发生器”（信号发生器）、负载编码器和加密数据通道后面，使检测

更加复杂。由于必须为每一种攻击的变体制作一个新的签名，而且随着规则的增加监测系统的运行速度将减缓，因此，签名引擎检测这些变化的攻击的整体能力将受到影响。

实际上，基于签名的入侵检测系统可以归结为攻击者和入侵检测系统签名开发商之间的竞赛，这场竞赛的关键是签名编写和应用到入侵检测引擎中的速度。

11.3.3　协议分析检测技术

在协议分析中，网络入侵检测系统的传感器检查 TCP 和 UDP 的有效荷载，且可以将其完全解码。协议分析提供了一种高级的网络入侵解决方案，可以检测更广泛的攻击，包括已知和未知的。

协议分析可以应用在不同的上层协议上（如 Telnet、FTP、HTTP、SMTP、SNMP、DNS等）对每一个用户命令作出详细分析，如果出现 IP 碎片设置，数据包将首先被重装，然后通过详细分析来了解潜在的攻击行为。通过重装数据包，系统可以检测到利用 IDS 逃避技术的攻击手段。

另外，协议分析与命令解析带来的好处是，当系统提升协议栈来解析每一层时，它用已获得的知识来消除在数据包结构中不可能出现的攻击。比如传输层协议是 TCP，那么将不用再搜索其他传输层协议如 UDP 上形成的攻击。如果数据包中的应用层协议是 SNMP，将不用再寻找 Telnet 或 HTTP 攻击。这样做的结果是性能得到明显改善。

协议解析也大大降低了模式匹配 IDS 系统中常见的误报现象。当数据包的一些字符串符合攻击特征库时系统就会报警，但该字符串实际上根本不是一个攻击，则属于误报。这样的误报不会在基于协议分析和命令解析的 IDS 系统中发生，因为它们知道和每个协议有关的潜在攻击的确切位置。

基于协议分析和命令解析的 IDS 网络传感器，采用高性能数据包驱动器，使其不仅支持线速百兆流量检测，而且千兆网络传感器具有 900 兆网络流量的 100%检测能力，可以支持 300 万个并发连接。

目前，国际优秀的 IDS 主要以模式发现技术为主，并结合异常发现、协议分析技术，即一个完备的入侵检测系统 IDS 一定是基于主机和基于网络两种方式兼备的分布式系统。

11.3.4　网管心得——无线入侵检测系统

随着黑客技术的提高，无线局域网（VLANS）受到越来越多的威胁。例如，配置无线基站（WAPS）的失误导致会话劫持以及拒绝服务攻击都将影响着无线局域网的安全。无线网络，有时基于传统有线网络 TCP/IP 架构而受到攻击，还可能受到基于电气和电子工程师协会（IEEE）发行 802.11 标准本身的安全问题而受到威胁。为了更好地检测和防御这些潜在的威胁，无线局域网也使用了一种入侵检测系统来解决这个问题。在此，将讲述为什么需要无线入侵检测系统、使用无线入侵检测系统的优点等。

1. 使用无线入侵检测系统原因

无线局域网容易受到各种各样的威胁，如 802.11 标准的加密方法和有线对等保密（Wired

Equivalent Privacy）都很脆弱。在“Weaknesses in the Key Scheduling Algorithm of RC-4”文档里就说明了 WEP key 能在传输中通过暴力破解攻击。即使 WEP 加密被用于无线局域网中，黑客也能通过解密得到重要数据。

黑客通过欺骗（rogue）WAP 得到重要数据。无线局域网的用户在不知道时，则认为自己通过很好的信号连入无线局域网，却不知已经遭到黑客的监听。随着低成本和易于配置造成了现在的无线局域网的流行，许多用户也可以在自己的传统局域网架设无线基站，随之而来的一些用户在网络上安装的后门程序，也造成了对黑客开放的不利环境，这正是没有配置入侵检测系统的组织机构开始考虑配置 IDS 的解决方案的原因。或许架设无线基站的传统局域网用户也同样面临着遭到黑客的监听的威胁。

基于 802.11 标准的网络还有可能遭到拒绝服务攻击的威胁，从而使得无线局域网难以工作。无线通信由于受到一些物理上的威胁会造成信号衰减，这些威胁包括树、建筑物、雷雨和山峰等破坏无线通信的物体。如微波炉、无线电话也可能威胁基于 802.11 标准的无线网络；黑客通过无线基站发起的恶意的拒绝服务攻击会造成系统重启。另外，黑客还能通过上文提到的欺骗 WAP 发送非法请求来干扰正常用户使用无线局域网。

还有一种威胁无线局域网的技术是 ever-increasing pace。这种威胁确实存在，并可能导致大范围的破坏，这也正是让 802.11 标准越来越流行的原因。对于这种攻击，现在暂时还没有好的防御方法，但将来会提出一个更好的解决方案。

2. 无线入侵检测系统优点

入侵检测系统通过分析网络中的传输数据来判断破坏系统和入侵事件。传统的入侵检测系统，仅能检测和对破坏系统作出反应。现在，入侵检测系统已用于无线局域网来监视分析用户的活动，判断入侵事件的类型，检测非法的网络行为，对异常的网络流量进行报警。

无线入侵检测系统同传统的入侵检测系统类似。但无线入侵检测系统加入了一些无线局域网的检测和对破坏系统反应的特性。

无线入侵检测系统可以通过提供商来购买，为了发挥无线入侵检测系统优良的性能，他们同时还提供无线入侵检测系统的解决方案。目前，市场上流行的无线入侵检测系统有 Airdefense RogueWatch 和 Airdefense Guard。与传统入侵检测系统相比存在如下优点。

- **架构**

从构架上来讲，无线入侵检测系统分为集中式和分散式两种。集中式无线入侵检测系统通常用于连接单独的 sensors（传感器），搜集数据并转发到存储和处理数据的中央系统中。分散式无线入侵检测系统通常由多种设备来完成 IDS 的处理和报告功能。但在实际应用中，分散式无线入侵检测系统比较适合较小规模的无线局域网，因为它价格便宜和易于管理。当需要过多的 sensors 时，拥有数据处理功能的 sensors 将不需要任何花费。所以，多线程的处理和报告的 sensors 管理比集中式无线入侵检测系统花费更多的时间。

无线局域网通常被配置在一个相对较大的环境中，若要更好地接收信号，也可配置多个无线基站，然后在无线基站的位置上部署 sensors，这样将提高信号的覆盖范围。由于这种物理架构，大多数的黑客行为会被检测到。另外，加大了同无线基站的距离，从而更好地定位黑客的详细地理位置。

- **策略执行**

无线入侵检测系统不但能找出入侵者，还能加强策略。通过使用强有力的策略会使无线局域网更安全。

❑ **威胁检测**

无线入侵检测系统，能检测出攻击者的行为，还能检测到 rogue WAPS，识别出未加密的 802.11 标准的数据流量。

为了更好地发现潜在的 WAP 目标，黑客通常使用扫描软件，如 Netstumbler 和 Kismet 这些软件；使用全球卫星定位系统（Global Positioning System）来记录他们的地理位置，这些工具正是因为许多网站对 WAP 地理支持而流行的。

比探测扫描更严重的是，无线入侵检测系统检测到的 DoS 攻击，DoS 攻击在网络上非常普遍。DoS 攻击都是因为建筑物阻挡造成信号衰减而发生的。黑客也喜欢对无线局域网进行 DoS 攻击。无线入侵检测系统能检测黑客的这种行为，如伪造合法用户进行泛洪攻击等。

另外，一些无线入侵检测系统，还能检测到 MAC 地址欺骗，然后通过数据分析，找出那些伪装 WAP 的无线上网用户。

11.4　IDS 的应用

防火墙和杀毒软件作为最早被用户接受的网络安全产品，已经成为安全方案中不可缺少的一部分。但是，仅仅依靠它们是远远不够的。IDS 作为全面安全产品体系的一部分，能保护重要的信息免受外部和内部的威胁。

11.4.1　IDS 设置

就像大多数复杂系统一样，为了最大限度地利用 IDS，必须事先制订大量的计划，设置相关策略，甚至在制订相应的策略之前就必须收集信息，对网络进行分析，同时还要对执行人员进行管理。通常，IDS 设置最为关键的是创建 IDS 策略，具体步骤依次分为定义 IDS 的目标、选择监视内容、选择对策、设置阈值和实现策略。

1. 定义 IDS 目标

IDS 目标提供策略的要求。潜在的目标包括攻击检测、防洪攻击、检测违反策略的情况、增强使用策略、增强连接策略和收集证据，且这些 IDS 目标可以是综合的，任何 IDS 的实际目标都取决于部署它的机构。这并不意味着它是一份综合的清单，IDS 可以让机构在攻击开始时发现攻击，并收集证据或通过终止事件来防止进一步的破坏。当然，这不是 IDS 可以提供的唯一服务，因为 IDS 会收集许多关于发生在网络和机构的计算机系统上的事件的详细信息，所以它还可以识别出违反策略的情况和网络资源的实际使用情况。

❑ **攻击识别**

攻击识别是 IDS 最常见的用途。编写 IDS 是为了查找某一类可能表明攻击正在进行的事件。一个简单的例子是连接到 TCP 端口 80（HTTP），其后跟有 URL，包括.bat 扩展。这表示入侵者正在试图攻击 IIS Web 服务器上的薄弱点。

大多数攻击的特征不是这么简单就可以被识别的。例如，在 Internet 上，仍然普遍使用的密码猜测攻击。HIDS 可能有一个规则，它用于查找短时间内针对每一个账号的 3 次失败的登录企图。为了实现这一点，HIDS 必须跟踪日志上显示的时间和每一个账号上失败的登录企图，

并且应该在登录成功或时间超时的时候重置其计时器。

一个更复杂的攻击识别的例子是，入侵者试图猜测多个账号和系统的密码。在这种情况下，攻击者可能不会连续两次尝试同一个账号，而是使用一个密码尝试进入在多个系统上发现的每一个账号。如果每一次尝试企图的时间足够长，那么攻击者在一个账号上 3 次失败所花费的时间就可能使计时器超时。唯一可以识别这种攻击的方法是将从不同系统上的日志收集到的信息联系在一起。

❑ **策略监视**

策略监视是攻击检测中一个不容易引人注意的目标。将一个 IDS 配置为进行策略监视的目的就是跟踪检查符合或不符合机构策略的情况。在最简单的情况下，可以将一个 NIDS 配置为跟踪所有流出网络的 Web 通信数据。这种配置允许 NIDS 跟踪所有不符合 Internet 使用的策略的情况。如果设置了一组不符合机构使用标准的 Web 站点，那么 NIDS 可以标记出所有到这些站点的连接。

NIDS 还可以检查路由器或防火墙配置。在这种情况下，NIDS 被配置为查找路由器或防火墙不允许通过的通信数据。如果发现了任何这种通信数据，则表明违反了公司防火墙策略。

❑ **策略增强**

将 IDS 作为策略增强工具需要对策略监视进行进一步的配置。对于策略增强，IDS 被配置为在发现违反策略的情况时采取行动。在“策略监视”的第一个例子中，策略增强 IDS 不会只是识别出连接到被接受的 Web 站点的企图，它还要采取行动阻止这种连接。

❑ **应急响应**

IDS 不仅可用于发现突发事件，而且在突发事件发生之后，也可以被用作收集证据和进行记录的工具。为了发挥这种作用，NIDS 可能被设置为查找某种连接并提供完整的通信数据记录。同时，HIDS 可能被配置为保留与系统特定账号相关的所有日志条目的记录。

2. 选择监视内容

选择监视内容是由 IDS 的目的和 IDS 的工作环境决定的。例如，如果 IDS 的目的是检测攻击，且位于公司防火墙外部的 Internet 上，则需要 IDS 监视进入防火墙的所有通信数据，以便发现进入的攻击。另一种情况，IDS 可能位于防火墙内部，只是为了识别所有成功入侵防火墙的攻击，在这种情况下，应该忽略流出的通信数据，如图 11-4 所示。

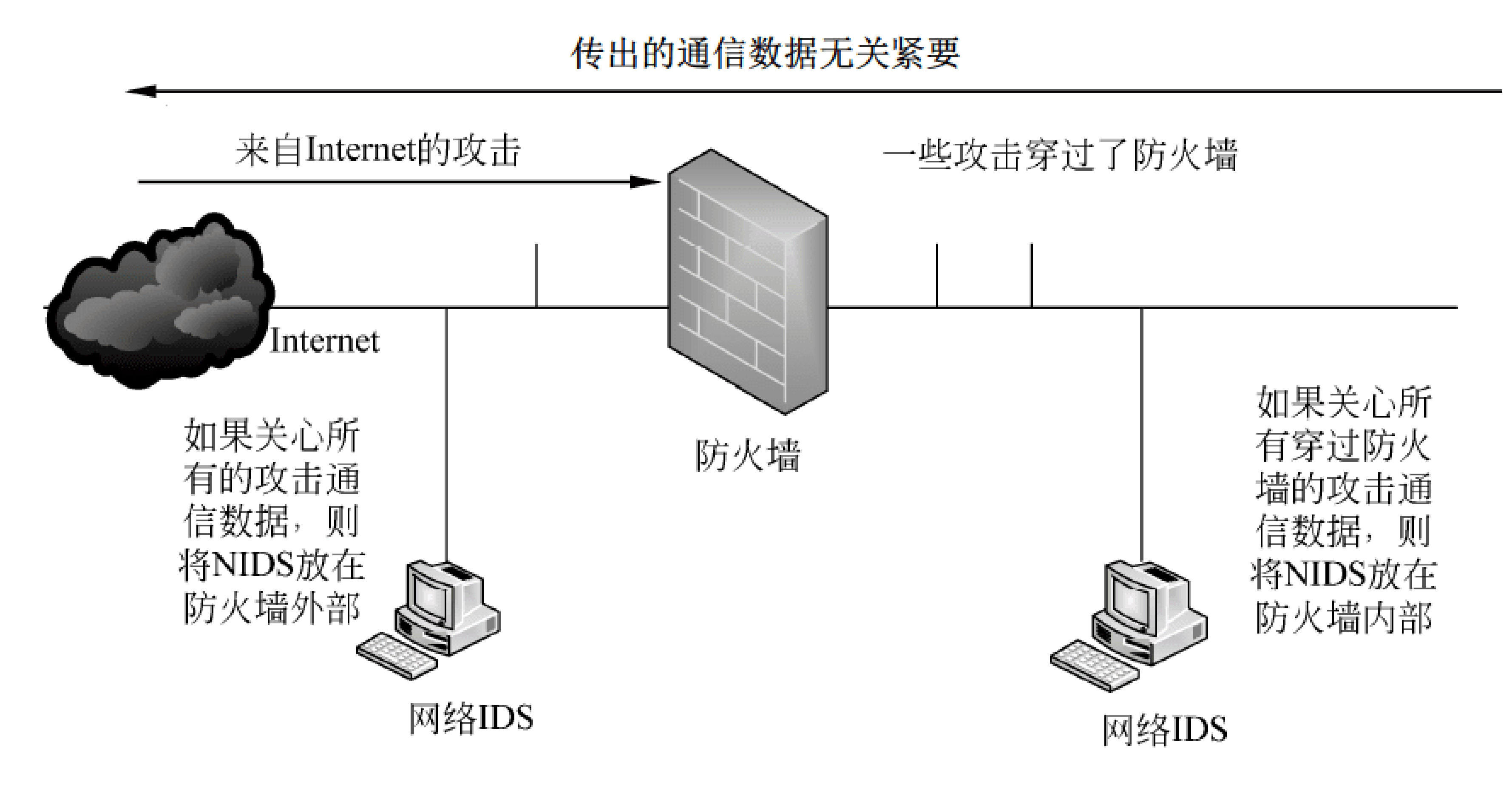


图 11-4　选择监视内容的例子

表 11-1 提供了在特定策略下监视内容的例子。

表 11-1　监视特定 IDS 策略的信息的示例

策略	NIDS	HIDS
攻击检测	进入潜在目标系统的所有通信数据（防火墙、Web 服务器、应用服务器等）	不成功的登录企图 连接企图 从远程系统的成功登录
防洪攻击	与攻击检测相同	与攻击检测相同
检测策略违反情况	来自客户系统的所有 HTTP 通信数据 来自客户系统的所有 FTP 通信数据 已知游戏端口的连接	成功的 HTTP 连接 成功的 FTP 连接 文件下载
使用策略的增强	与检测策略违反情况相同	与检测策略违反情况相同
增强连接策略	增强违反连接策略的所有通信数据	从禁止的地址或端口发出的成功连接

对监视内容的选择将决定检测器的位置。可以将检测器放在防火墙之外、内部网络中、敏感系统或专门用来收集和处理日志文件的系统上。在确定 IDS 检测器的位置时，要记住的关键一点是检测器必须可以从网络通信数据或日志条目中发现值得注意的事件。如果值得注意的事件不会通过防火墙，那么将 NIDS 检测器放在防火墙内就不是一种好的选择。同样，如果只在 Windows NT 网络的主域控制器上记录值得注意的事件，则必须将 HIDS 软件安装在主域控制器上，即使攻击者可能实际位于网络某处的工作站上，也应该如此。

3．选择响应方式

与选择监视内容一样，选择如何响应是由 IDS 的目的决定的。当事件发生时，可以选择被动地响应（一种不直接阻止攻击者行动的响应），也可以选择主动响应（试图直接阻止攻击者行动的响应）。被动响应并不意味着让事件继续，而是选择不让 IDS 本身采取直接行动，同时还要权衡选择自动响应还是人工响应。

4．设置临界值

临界值为误报提供了保护，加强了 IDS 策略的整体有效性。临界值用于从有目的的事件中过滤掉突发事件。例如，一位员工可能通过搜索引擎所提供的链接连接到一个与业务无关的 Web 站（该员工可能进行了合法的搜索，但是由于搜索参数有误而返回了不合适的 Web 站点）。在这种情况下，单一事件可能不会造成 IDS 发送报告，只会在调查无害的行为上浪费资源。

同样，应该将检测攻击的临界值设置为忽略低级别的检测或单个信息收集事件。这种事件可能包括了一个检索（Finger）员工的企图。Finger 是一个 UNIX 系统中的常见程序，经常被用来检查正确的邮件地址或获得公钥。

IDS 的合适临界值的选择直接取决于可能出现的事件类型和违反策略的类型。不可能给出一组普遍适用的绝对临界值。不过，可以找出一组在设置临界值时必须考虑的参数。这些参数包括以下几种。

- **用户技术级别**　大量的用户错误可以造成大量的错误警报。
- **网络速度**　对于需要某些数据包在特定时间内出现的事件而言，低速网络可以造成错

误的警报。

- **预期的网络连接** 如果将 IDS 配置为对某些将在正常情况下出现的网络连接报警，那么就会产生大量的错误报警。
- **管理员/安全负责人的工作负荷** 安全人员的高负荷可能需要很高的临界值，以减少错误报警的次数。
- **检测器敏感度** 如果检测器非常敏感，则需要将临界值设置得高一些，以避免产生大量的错误报警。
- **安全程序的有效性** 如果机构的安全程序非常有效，那么即使 IDS 漏掉一些攻击也是可以接受的，因为在网络中还存在其他防御手段。
- **现有的薄弱点** 没有理由对网络上不存在的薄弱点实施的攻击进行报警。
- **系统和信息的敏感度** 机构中使用的信息越敏感，警报的临界值就应该设置得越低。
- **误报的后果** 如果误报的后果非常严重，则应该将临界值设置得高一些，从而减少错误指示。
- **漏报的后果** 相反，如果漏报（或漏掉事件）的后果非常严重，则应该将临界值设置得低一些。

临界值是与机构密切相关的。虽然可以提供一般性的指导，但是每个机构都必须根据上面提供的参数确定自己的临界值。

5. 实现系统

一旦制订了 IDS 策略并得出初始的临界值设置，就应该安放带有最终策略的 IDS，并减少当前措施。在一段时间内应该对 IDS 进行严密的监视，以评估临界值。这样，就可以获得对策略的经验而不会干扰正常的网络通信或计算机连接。

同样重要的是，在该试验阶段，应该小心进行 IDS 所做的任何调查，注意评估 IDS 所提供的信息的准确性。

11.4.2 IDS 部署

基于主机的 IDS 比较准确，而基于网络的 IDS 更及时，综合部署这两种 IDS 能给网络带来更大的安全性。

首先，部署一个基础的混合型入侵检测系统时，应把基于网络的入侵检测安装于网络信息集中通过的地方如中心交换机、集线器等上面，对所有通过的网络数据进行收集、分析，并对攻击行为作出响应。而基于主机的入侵检测系统应安装于受保护的主机上，收集信息，对主机攻击行为作出响应。

联合使用基于主机和基于网络两种方式，会达到更好的检测效果。比如基于主机的 IDS 使用系统日志作为检测依据，因此它们在确定攻击是否已经取得成功时与基于网络的检测系统相比具有更高的准确性。人们完全可以使用基于网络的 IDS 提供早期报警，而使用基于主机的 IDS 来验证攻击是否取得成功。在下一代的入侵检测系统中，将把现在的基于网络和基于主机这两种检测技术很好地集成起来，提供集成化的攻击签名、检测、报告和事件关联功能。

其次，部署基于硬件的入侵检测系统应并联在网络中，通过旁路监听的方式实时地监视

网络中的流量。这样能对网络的运行和性能无任何影响地判断其中是否含有攻击的企图，并通过各种手段向管理员报警，不但可以发现来自外部的攻击，也可以发现内部的恶意行为。

小型网络的 IDS 部署如图 11-5 所示。网络安全由 IDS 检测引擎、IDS 管理主机两部分组成。检测引擎在检测到攻击时，引擎能即刻作出响应，如进行告警/通知（向控制台告警、向安全管理员发 E-mail、SNMP Trap、查看实时会话和通报其他控制台），记录现场（记录事件日志及整个会话），采取安全响应行动（终止入侵连接、调整网络设备配置如防火墙、执行特定的用户响应程序）。IDS 管理主机则可以接受实时报警，查询引擎中的数据，进行统计分析。

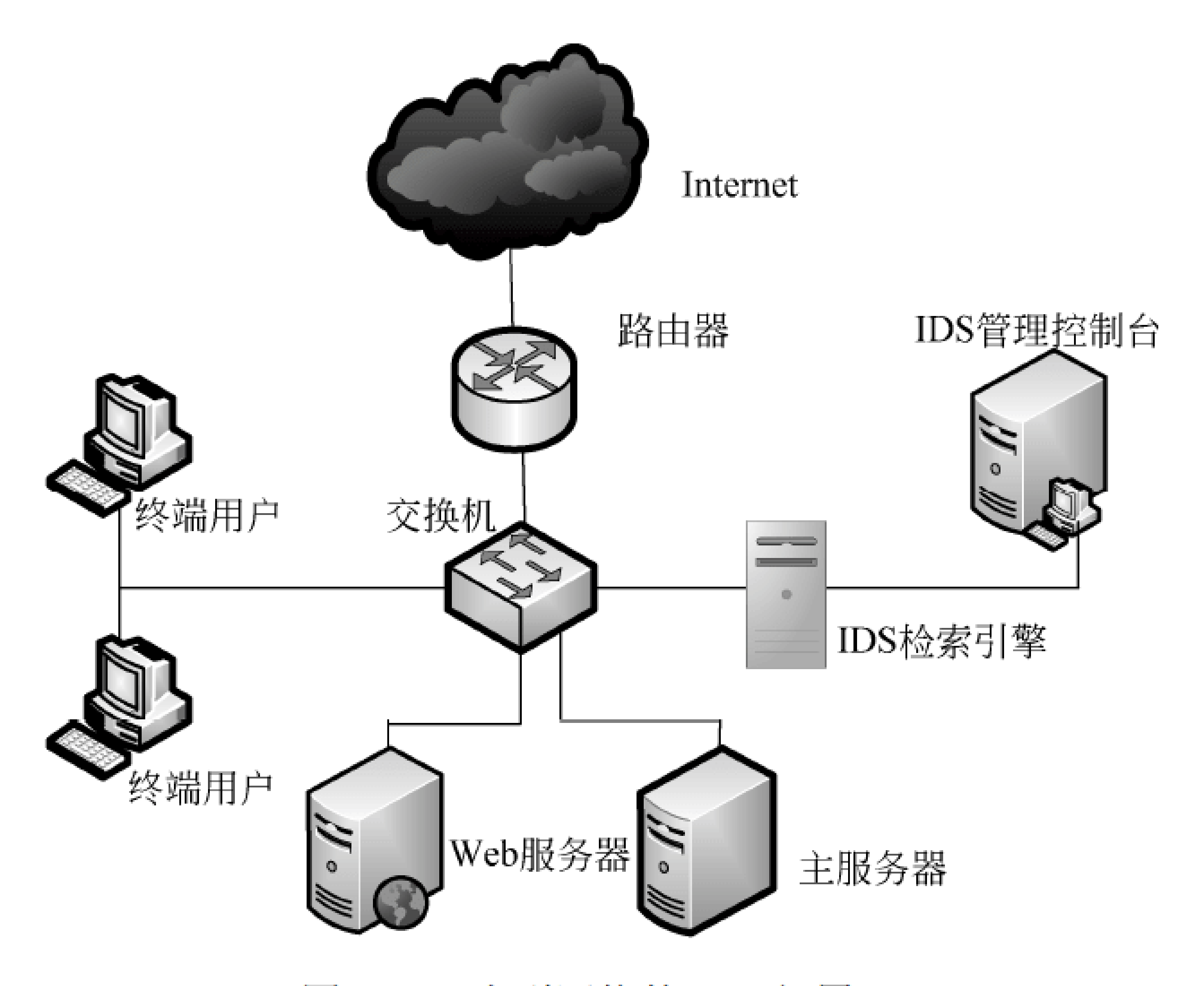


图 11-5　小型网络的 IDS 部署

在大中型网络的安全建设中，应增设检测引擎中心机，如图 11-6 所示。这是由于大中型网络的拓扑结构复杂，地域分布广，数据流量大，需要使用多个引擎才能对整个网络进行监控。对此专门增设一台中心机，由它负责收集和保存各引擎检测到的数据，并进行二次分析，为管理员提供综合分析报告。管理员的指令也可以通过中心机自动下发到各引擎中去执行，从而提高管理效率。

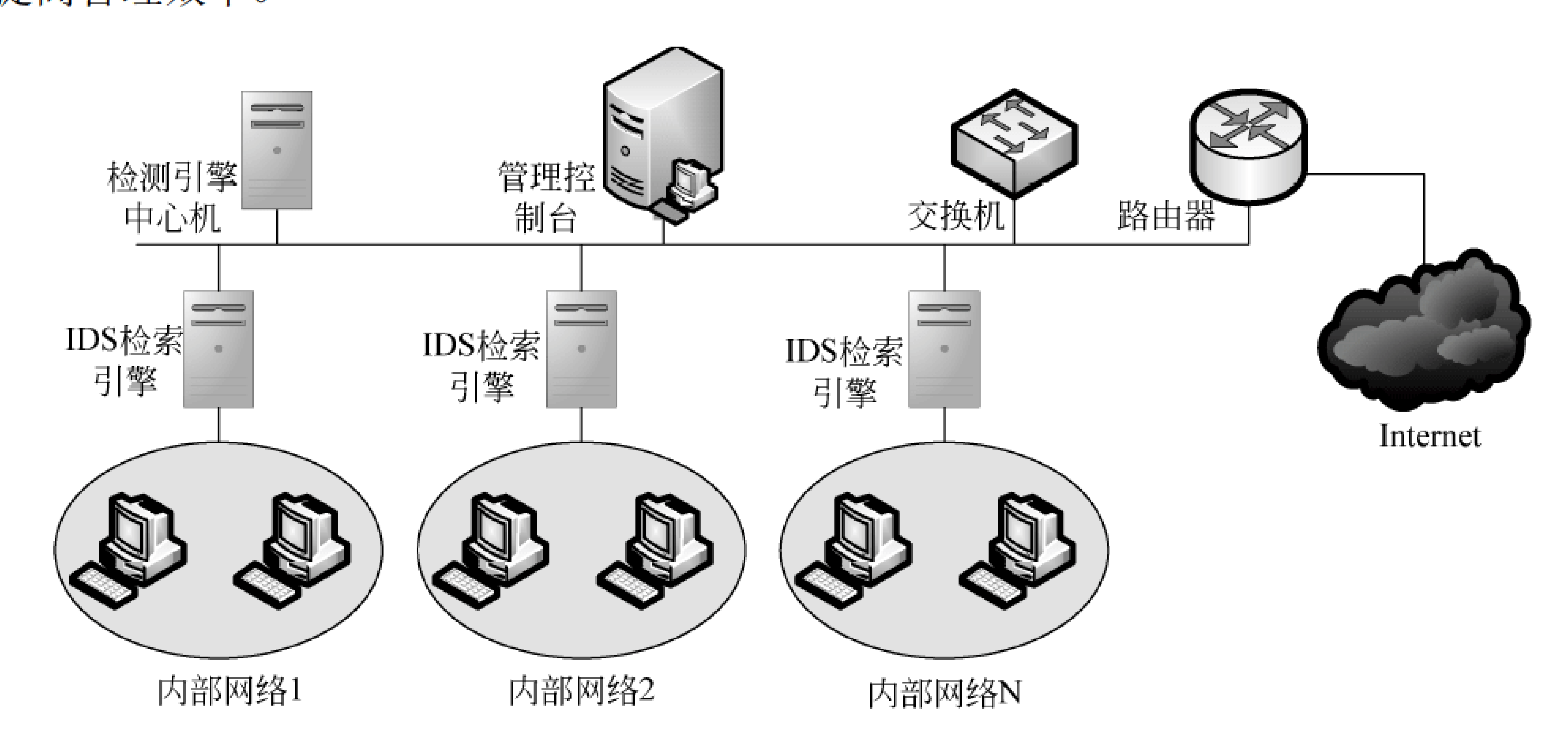


图 11-6　大型网络 IDS 的部署

目前，大部分的 IDS 产品由入侵检测引擎和管理控制台组成，在具体应用时可以根据网络结构和需求做不同的部署。一般是部署在需要重点保护的部位，如企业内部重要服务器所在的子网，对该 IDS 的发展趋势网中的所有连接进行监控。根据网络的拓扑结构的不同，入侵检测系统的监听端口可以接在共享媒质的集线器或交换机的镜像端口（SpanPort）上，或专为监听所增设的分接器（Tap）上。

11.4.3 网管心得——如何构建一个基于网络的 IDS

通常，一个企业或机构在准备构建入侵检测系统时，往往选择从基于网络的 IDS 入手，因为网上有很多这方面的开放源代码和资料，实现起来比较容易，且适应能力强。有了简单网络 IDS 的开发经验，再向基于主机的 IDS、分布式 IDS、智能 IDS 等方面迈进的难度就小了很多。在此，以基于网络的 IDS 为例，介绍典型的 IDS 开发思路。

根据 CIDF 规范，可从功能上将入侵检测系统划分为 4 个基本部分：数据采集子系统、数据分析子系统、控制台子系统、数据库管理子系统。

具体实现起来，一般都将数据采集子系统（又称探测器）和数据分析子系统在 Linux 或 UNIX 平台上实现，称之为数据采集分析中心；将控制台子系统在 Windows 平台上实现，数据库管理子系统基于 Access 或其他功能更强大的数据库，多跟控制台子系统结合在一起，称之为控制管理中心。在此以 Linux 和 Windows Server 2008 平台为例介绍数据采集分析中心和控制管理中心的实现，并按照如下步骤构建一个基于网络的入侵检测系统。

1. 获取 libpcap 和 tcpdump

审计踪迹是 IDS 的数据来源，而数据采集机制是实现 IDS 的基础，否则入侵检测就无从谈起。

数据采集子系统位于 IDS 的最底层，其主要目的是从网络环境中获取事件，并向其他部分提供事件。目前比较流行的做法是使用 libpcap 和 tcpdump 检测工具，将网卡置于“混杂”模式，捕获某个网段上所有的数据流。

libpcap 是 UNIX 或 Linux 从内核捕获网络数据包的必备工具，它是独立于系统的 API 接口，为底层网络监控提供了一个可移植的框架，可用于网络统计收集、安全监控、网络调试等应用。tcpdump 是用于网络监控的工具，可能是 UNIX 上最著名的 sniffer 了，它的实现基于 libpcap 接口，通过应用布尔表达式打印数据包首部，具体执行过滤转换、包获取和包显示等功能。tcpdump 可以描述系统的正常行为，并最终识别出那些不正常的行为，当然，它只是益于收集关于某网段上的数据流（网络流类型、连接等）信息，至于分析网络活动是否正常，则是程序员和管理员所要做的工作。

libpcap 和 tcpdump 在网上广为流传，开发者可以到相关网站下载。

2. 构建并配置探测器，实现数据采集功能

首先应根据自己网络的具体情况，选用合适的软件及硬件设备，如果网络数据流量很小，用一般的计算机安装 Linux 即可，如果所监控的网络流量非常大，则需要用一台性能较高的计算机。接着，在 Linux 服务器上开出一个日志分区，用于采集数据的存储。

其次，创建 libpcap 库。从网上下载的通常都是 libpcap.tar.z 的压缩包，所以应先将其解压缩、解包，然后执行配置脚本，创建适合于自己系统环境的 Makefile，再用 make 命令创建 libpcap 库。libpcap 安装完毕之后，将生成一个 libpcap 库、三个 include 文件和一个 man 页面（即用户手册）。

然后，创建 tcpdump。与创建 libpcap 的过程一样，先将压缩包解压缩、解包到与 libpcap 相同的父目录下，然后配置、安装 tcpdump。如果配置、创建、安装等操作一切正常的话，此时，系统已经能够收集到网络数据流了。

3. 建立数据分析模块

网上有一些开放源代码的数据分析软件包，这给构建数据分析模块提供了一定的便利条件，但同时有很大的局限性，要开发一个真正功能强大、实用的 IDS，通常都需要开发者自己动手动脑设计数据分析模块，这也是整个 IDS 的工作重点。

数据分析模块相当于 IDS 的大脑，它必须具备高度的“智慧”和“判断能力”。所以，在设计此模块之前，开发者需要对各种网络协议、系统漏洞、攻击手法、可疑行为等有一个很清晰、深入的研究，然后制定相应的安全规则库和安全策略，再分别建立滥用检测模型和异常检测模型，让机器模拟自己的分析过程，识别确知特征的攻击和异常行为，最后将分析结果形成报警消息，发送给控制管理中心。

设计数据分析模块的工作量很大，且考虑到黑客攻击手段日益翻新，所以，这注定是一个没有终点的过程，需要不断地更新、升级、完善。在这里需要特别注意 3 个问题。

- 应优化检测模型和算法的设计，确保系统的执行效率。
- 安全规则的制定要充分考虑包容性和可扩展性，以提高系统的伸缩性。
- 报警消息要遵循特定的标准格式，增强其共享与互操作能力，切忌随意制定消息格式的不规范做法。

4. 构建控制台子系统

控制台子系统负责向网络管理员汇报各种网络违规行为，并由管理员对一些恶意行为采取行动（如阻断、跟踪等）。由于 Linux 或 UNIX 平台在支持界面操作方面远不如常用的 Windows 产品流行，所以为了把 IDS 做成一个通用、易用的系统，笔者建议将控制台子系统在 Windows 系列平台上实现。

控制台子系统的主要任务有两个。

- 管理数据采集分析中心，以友好、便于查询的方式显示数据采集分析中心发送过来的警报消息。
- 根据安全策略进行一系列的响应动作，以阻止非法行为，确保网络的安全。

控制台子系统的设计重点是：警报信息查询、探测器管理、规则管理及用户管理。

- **警报信息查询** 网络管理员可以使用单一条件或复合条件进行查询，当警报信息数量庞大、来源广泛时，系统需要对警报信息按照危险等级进行分类，从而突出显示网络管理员需要的最重要信息。
- **探测器管理** 控制台可以一次管理多个探测器（包括启动、停止、配置、查看运行状态等），查询各个网段的安全状况，针对不同情况制定相应的安全规则。

- **规则库管理功能** 为用户提供一个根据不同网段具体情况灵活配置安全策略的工具，如一次定制可应用于多个探测器、默认安全规则等。
- **用户管理** 对用户权限进行严格的定义，提供口令修改、添加用户、删除用户、用户权限配置等功能，有效保护系统使用的安全性。

5．构建数据库管理子系统

一个好的入侵检测系统，不仅仅为管理员提供实时、丰富的警报信息，还应详细地记录现场数据，以便于日后需要取证时重建某些网络事件。

数据库管理子系统的前端程序，通常与控制台子系统集成在一起，用 Access 或其他数据库存储警报信息和其他数据。该模块的数据来源有两个：一是数据分析子系统发来的报警信息及其他重要信息；二是管理员经过条件查询后对查询结果处理所得的数据，如生成的本地文件、格式报表等。

6．联调

以上几步完成之后，一个 IDS 的最基本框架已被实现。但要使该 IDS 顺利地运转起来，还需要保持各个部分之间安全、顺畅地通信和交互，这就是联调工作所要解决的问题。

首先，要实现数据采集分析中心和控制管理中心之间的通信，两者之间是双向的通信。控制管理中心显示、整理数据采集分析中心发送过来的分析结果及其他信息，数据采集分析中心接收控制管理中心发来的配置、管理等命令。注意确保两者之间通信的安全性，最好对通信数据流进行加密操作，以防被窃听或篡改。同时，控制管理中心的控制台子系统和数据库子系统之间也有大量的交互操作，如警报信息查询、网络事件重建等。

联调通过之后，一个基本的 IDS 就搭建完毕。后面要做的就是不断完善各部分功能，尤其是提高系统的检测能力。

11.5 IDS 的发展方向

IDS 作为网络安全架构中的重要一环，其重要地位有目共睹。随着技术的不断完善和更新，IDS 正呈现出新的发展态势。IPS（入侵防御系统）的出现，应该说是 IDS 技术的一种新发展趋势。IPS 技术在 IDS 监测的功能上又增加了主动响应的功能，一旦发现有攻击行为则立即响应，主动切断连接。

除了 IPS，也有厂商提出了 IMS（入侵管理系统）。IMS 是一个过程，它在入侵行为未发生前要考虑网络中有什么漏洞，判断有可能会形成什么攻击行为和面临的入侵危险；在行为发生时或即将发生时，检测出入侵行为，并主动阻断、终止入侵行为；在入侵行为发生后，还要深层次分析入侵行为，通过关联分析，来判断是否还会出现下一个攻击行为。IMS 符合 IDS 向管理系统发展的方向，也是 IDS 未来的一个发展方向。综合这些新的发展动态，可以了解未来 IDS 的发展趋势将表现如下总体特征。

1．智能化

入侵检测系统的核心是分析能力。未来的入侵检测系统应该能够进行基于事件语义而不

是基于事件语法的检测，这种方法将弥补当前在安全政策和检测政策之间的差距，是对当前检测办法的一个极大的改进。在当前的检测中，检测目标需要复杂的、特定的与操作系统相关的检测特征。

2. 分布式

随着网络攻击手段向分布式方向发展（如目前出现的分布式拒绝服务攻击 DDoS），且采用了各种数据处理技术，其破坏性和隐蔽性也越来越强。相应地，入侵检测系统也在向分布式结构发展，采用分布收集信息、分布处理、多方协作的方式，将基于主机的 IDS 和基于网络的 IDS 结合使用，构筑面向大型网络的 IDS。其中的关键技术是协作式入侵检测技术，包括同一系统中不同入侵检测部件之间的协作，尤其是主机型和网络型入侵检测部件之间的协作，以及异构平台之间、不同安全工具之间的协作、不同厂家的安全产品之间的协作。

3. 高速网络环境下的入侵检测

截获网络的每一个数据包，并分析、匹配其中是否具有某种攻击的特征需要花费时间和系统资源。随着网络带宽的增大，1000MB 以太网、光纤技术的大量应用使得网络入侵检测系统的处理能力跟不上处理需求，因此，在高速网络环境中进行入侵检测是当前迫切需要解决的问题。

4. 基于硬件的入侵检测

基于硬件的入侵检测系统和安全网络工具箱集成在一起也是一个趋势，这种设备定位于家庭市场和小企业市场，以使客户能够处理与持续地连接到 Internet 上相关的问题。

总之，入侵检测是一门综合性技术，既包括实时检测技术，也有事后分析技术。由于攻击的天然不确定性，单一的 IDS 产品可能无法做到面面俱到。因此，IDS 的未来发展必然是多元化的。只有通过不断改进和完善技术，才能更好地协助网络进行安全防御。

11.6 操作实例

11.6.1 操作实例——使用 Sax 入侵检测系统

入侵检测系统是一种积极主动的网络安全防护工具，它通过对网络中所有传输的数据进行智能分析和检测，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，在网络系统受到危害之前拦截和阻止入侵。

1. 实例目的

- ❑ 启用入侵检测系统。
- ❑ 检测网络状况。
- ❑ 防止网络入侵。

2. 实例步骤

（1）在一个网络中，有一台服务器和一台客户机，其 IP 分别是:“192.168.0.200”和“192.168.0.15”，拓扑结构示意图如图 11-7 所示。

（2）在服务器桌面双击 Sax 应用程序图标，在该程序的主界面中，单击【专家检测】按钮如图 11-8 所示。

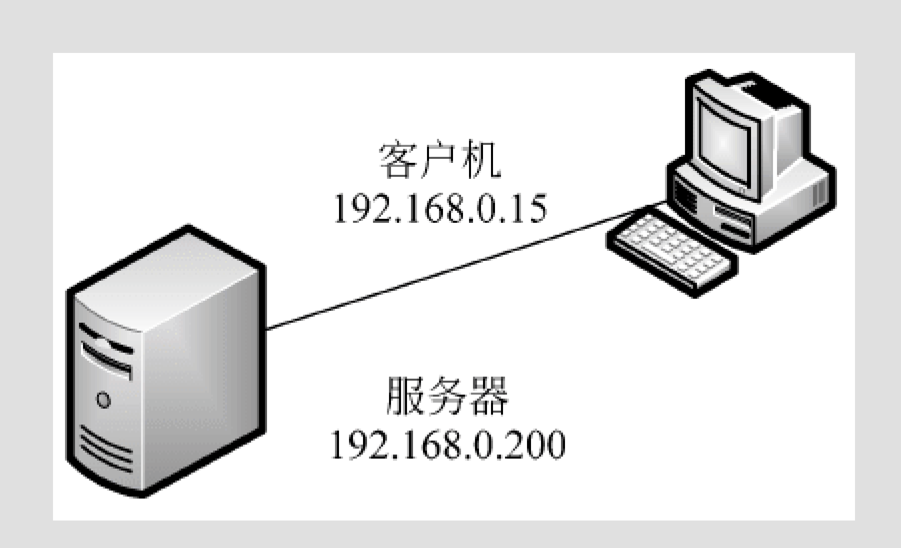


图 11-7　拓扑结构示意图

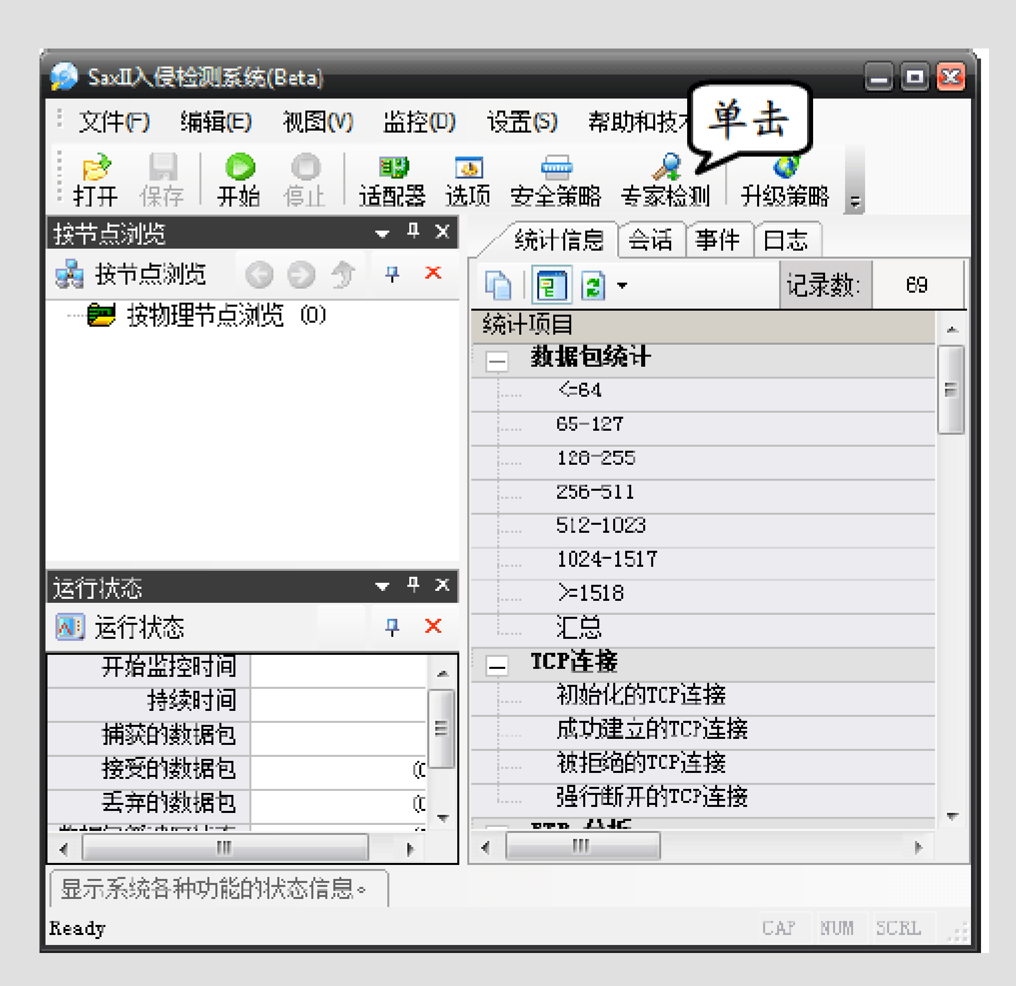


图 11-8　Sax 主界面

（3）在弹出的对话框的左侧窗格中，展开 ICMP 节点，启用【ICMP_Ping 事件】复选框，并单击【关闭】按钮，如图 11-9 所示。

（4）在 Sax 主界面中，单击【开始】按钮，如图 11-10 所示。





图 11-9　查看联机的磁盘

图 11-10　开始检测

（5）在弹出的对话框中，启用 Intel（R）PRO/1000 MT Network Connection 复选框，并单

击【确定】按钮，如图 11-11 所示。

（6）在客户机桌面执行【开始】|【运行】命令，在弹出的对话框中输入 cmd 命令，并单击【确定】按钮，如图 11-12 所示。



图 11-11　启用计算机网卡

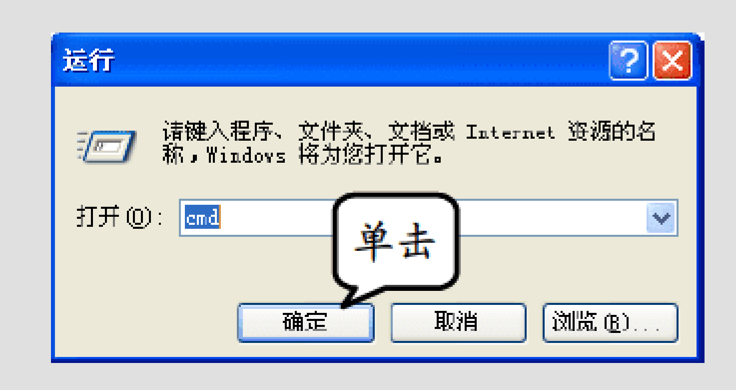


图 11-12　运行 cmd 命令

（7）在【命令提示符】窗口中输入 ping –t 192.168.0.200（不断地对服务器进行泛红 ping）命令，如图 11-13 所示。

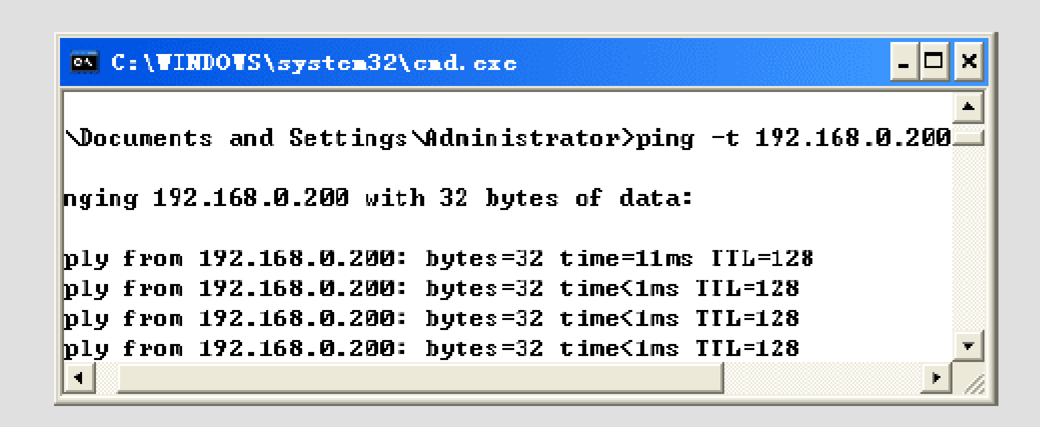


图 11-13　命令提示符

（8）在 Sax 主界面中，单击【停止】按钮（停止检测）。在右方窗格中，选择【会话】选项卡（检测到客户机对服务器的防洪会话），如图 11-14 所示。

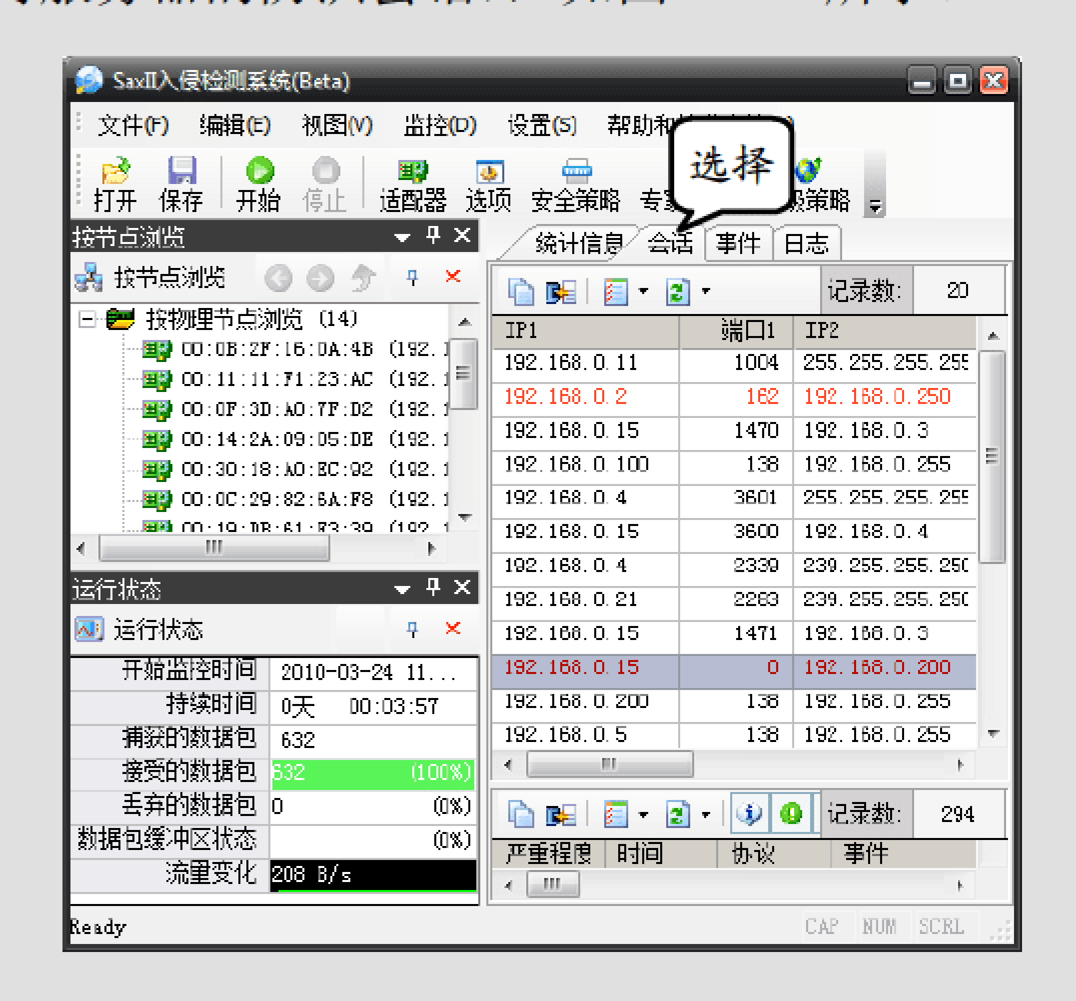


图 11-14　查看会话记录



查看【事件】选项卡，可以看到 ICMP-PING 事件，证明了入侵检测系统可以检测出网络被攻击的迹象。

第五篇　加密技术及备份技术

第12章 公钥基础设施

随着资源共享的进一步加强，随之而来的信息安全问题也日益突出。而身份认证、权限和访问控制又是网络应用安全的两个重要内容，身份认证与访问控制的使用，能很好地保证系统的安全性、可访问性和稳定性。目前，公钥基础设施 PKI（Public Key Infrastructure）在国内外已经得到广泛的应用。如安全电子邮件、Web 访问、虚拟专用网络 VPN 和本地简单登录认证，以及电子商务、电子政务、网上银行和网上证券交易等各种强认证系统都普遍应用了 PKI 技术。

公钥基础设施是利用公钥概念和加密技术为网上通信提供的符合标准的一整套安全基础平台。公钥基础设施能为各种不同安全需求的用户提供各种不同的网上安全服务，主要有身份识别与鉴别（认证）、数据保密性、数据完整性、不可否认性及时间戳服务等。用户利用 PKI 所提供的这些安全服务进行安全通信，以及不可否认的安全电子交易活动。

本章学习要点：

- PKI 基础
- PKI 服务和实现
- 熟悉 PKI 的体系结构
- 了解属性权威和权限管理
- 熟悉基于 PMI 建立的安全应用

12.1 PKI 基础

PKI 是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。

12.1.1 网络安全对于 PKI 的需求

随着网络技术和信息技术的发展，电子商务已逐步被人们所接受，并在不断普及。但由于各种原因，国内电子商务的安全性却不能得到有效的保障。在常规业务中，交易双方现场交易，可以确认购买双方的身份。利用商场开具的发票和客户现场支付商品费用，无须担心发生纠纷时无凭证可寻。但通过网上进行电子商务交易时，由于交易双方并不现场交易，因此，无法确认双方的合法身份，同时交易信息是交易双方的商业秘密，在网上传输时必须保

证安全性，防止信息被窃取；双方的交易非现场交易，一旦发生纠纷，必须能够提供仲裁。

因此，在电子商务中，必须从技术上保证双方在交易过程中能够实现身份认证、安全传输、不可否认性、数据完整性。在采用数字证书认证体系之前，交易安全一直未能真正得到解决。由于数字证书认证技术采用了加密传输和数字签名，能够实现上述要求，因此在国内外电子商务中，都得到了广泛的应用。

PKI 就是使用最广泛的信息安全技术之一。其原理是通过数学加解密的公式发展而成。利用数学加解密公式可制成两种数字钥匙。其中，一种钥匙叫公钥（Public Key）公开发行；另一种钥匙叫私钥（Private Key），由使用者自己保管。在通过第三方的可信任机构（认证机构，即 CA），把用户的公钥和用户的其他标识信息捆绑在一起，其中包括用户名和电子邮件地址等信息，以在 Internet 网上验证用户的身份，保证网络数据传输的安全。

因此，从大的方面来说，所有提供公钥加密和数字签名服务的系统，都可归结为 PKI 系统的一部分，PKI 的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性。



数据的机密性是指数据在传输过程中，不能被非授权者偷看；数据的完整性是指数据在传输过程中不能被非法篡改；数据的有效性是指数据不能被否认。

一个有效的 PKI 系统必须是安全的和透明的，用户在获得加密和数字签名服务时，不需要详细地了解 PKI 的内部运作机制。在一个典型、完整和有效的 PKI 系统中，除证书的创建和发布，特别是证书的撤销外，一个可用的 PKI 产品还必须提供相应的密钥管理服务，包括密钥的备份、恢复和更新等。密钥管理系统将极大影响一个 PKI 系统的规模、可伸缩性和在协同网络中的运行成本。在一个企业中，PKI 系统必须有能力为一个用户管理多对密钥和证书；能够提供安全策略编辑和管理工具，如密钥周期和密钥用途等。

PKI 作为一种安全技术，已深入到网络的各个层面，这从侧面反映了 PKI 强大的技术优势。其中，PKI 的优势主要表现为以下几点。

❑ 支持可公开验证并无法仿冒的数字签名

采用公开密钥密码技术，能够支持可公开验证并无法伪造的数字签名，从而在支持可追究的服务上具有不可替代的优势。这种可追究的服务也为原发数据完整性提供了更高级别的担保。支持公开验证，能更好地保护弱势个体，完善平等的网络系统间的信息和操作的可追究性。

❑ 保护机密性

由于密码技术的采用，保护机密性是 PKI 最突出的优点。PKI 不仅能为相互认识的实体之间提供机密性服务，同时也可以为陌生的用户之间的通信提供保密支持。

❑ 保证服务范围的无限制扩张

由于数字证书可以由用户独立验证，不需要在线查询，原理上能够保证服务范围无限制地扩张，这使得 PKI 能够成为一种服务巨大用户群的基础设施。PKI 采用数字证书方式进行服务，即通过第三方颁发的数字证书证明末端实体的密钥，而不是在线查询或在线分发。这种密钥管理方式突破了过去安全验证服务必须在线的限制。

❑ 应用领域不受具体应用限制

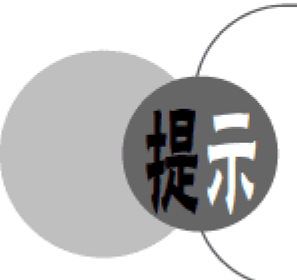
PKI 提供了证书的吊销机制，从而使得其应用领域不受具体应用的限制。吊销机制提供了在意外情况下的补救措施，在各种安全环境下都可以让用户更加放心。另外，因为有吊销技术，不论是永远不变的身份还是经常变换的角色，都可以得到 PKI 的服务而不用担心被窃后身份或角色被永远作废或被他人恶意盗用。

❑ 极强的互联能力

PKI 具有极强的互联能力。不论是上下级的领导关系，还是平等的第三方信任关系，PKI 都能够按照同样的信任方式进行多种形式的互联互通，从而使 PKI 能够很好地服务于大型网络信息系统。PKI 中各种互联技术的结合使建设一个复杂的网络信任体系成为可能。

12.1.2　认证机构和数字证书

在 PKI 中，认证机构（Certification Authority，CA）是负责创建或者证明身份的可信赖的权威机构。这远不止是运行一个能够生成用作电子身份的数字证书的应用程序那么简单。它们之间的区别就好像是颁发护照的国家护照管理局与能够复制护照的彩色影印服务之间的区别一样。也就是说能够创建身份并不意味着所有的人都会使用或者信任这些身份。



身份证明是指证实一个数字身份的申请者的初始（真实）身份的过程。在大多数 CA 实现中，这一功能都被单独划出来由注册机构(Registration Authority，RA）实现。

CA 实现了对申请注册证书的申请者的身份验证以及颁发可用于证明该身份的数字证书的过程。被颁发的身份有特定的有效期，该 CA 有能力撤销该证书并且通知证书使用者该证书已被撤销。

通常，人们会想到应该相信谁颁发的身份，它们颁发的身份所使用的步骤是什么，这些可以在日常生活中使用的身份证中找到先例。然而，对于创建那些用于电子世界身份的 CA，人们还会有应该信任哪些人运作的 CA、身份使用范围、确定那些身份需要使用的步骤及如何证明、采用何种机制来提供一种合理的不可伪造的身份等问题。

在寻找值得信任的 CA 运作者时，人们可能首先想到的就是可信赖机构。其中，包括银行、信用卡公司、邮局、政府部门（如税务局）或者护照管理局等。但是，这些组织并不一定都是 CA 运作者的合适人选。例如，交通部颁发的用于驾驶执照的电子证书是合理的，但是用户也许并不希望它们和自己的信用卡或者信誉评价扯上关系。

除了传统形式的可信赖实体之外，新形式的颁发证书的权威机构也已经出现。这些公共 CA 当中的许多都曾经不得不在没有事先存在的名声或者声誉可以利用的情况下建立可以信赖的名声。公共 CA 是通过建立十分安全的程序，小心地确立和审计操作过程以及操作人员从而建立起它们可以被信赖的名声。

数字证书是由权威机构——CA 证书授权（Certificate Authority）中心发行的，能提供在 Internet 上进行身份验证的一种权威性电子文档，人们可以在互联网交往中用它来证明自己的身份和识别对方的身份。

数字证书在一个身份和该身份的持有者所拥有的公/私密钥对之间建立一种联系。通常，人们可以信赖一个特定的颁发机构，由它根据用户所要达到的目标来确立身份。另外，还要生成一份可以证实用户已经获得了一个有效身份的文件。数字证书就是这一文件的电子形式。

在电子领域中，如果要使用“身份”的话，用户需要生成一份数字文件或者证书，这份文件或者证书应该提供足够的信息，使得他人能够相信你就是该身份的合法持有者。

认证中心所颁发的数字证书均遵循 X.509 V3 标准，其格式在 ITU 标准和 X.509 V3 中均有定义，图 12-1 为 X.509 证书的结构示意图，其中证书和级别信息采用 X.500 的可辨别名 DN 来标记，它是一个复合域，通过一个子组件来定义。

Version Number	
Serial Number	
Signature algorithm	
Issuer name	
Validity period	
Subject name	
Subject public key	V1 fields
Issuer unique identifier	
Subject unique identifier	V2 fields
Extensions	
Signature algorithm	V3 fields
Signature value	V1 fields

图 12-1　X.509 证书结构

- **版本号（Version Number）** 定义证书的版本号，这将最终影响证书中包含信息的类型和格式。目前版本 4 已发布，但在实际使用过程中版本 3 仍占主流。
- **序列号（Serial Number）** 序列号是赋予证书的唯一整数值，主要用于将证书与同一 CA 颁发的其他证书相区别。
- **签名算法标识（Signature algorithm）** 该域中含有 CA 签发证书所使用的数字签名算法的算法标识符，如 SHA1WithRSA，有 CA 的签名，便可以保证证书拥有者身份的真实性，而且 CA 也不能否认其签名。
- **颁发者 X500 名称（Issuer name）** 必选项。该域中含有签发证书实体的唯一名称（DN），命名必须符合 X.500 格式，通常为某个 CA。
- **证书有效期（Validity period）** 证书仅仅在一个有效的时间段内有效，证书的有效期就是该证书的有效时间段，该域表示两个日期的序列，即证书的有效开始日期（notBefore）和证书有效期结束的日期（notAfter）。
- **证书持有者 X500 名称（Subject name）** 必选项。即证书拥有者的可识别名称，命名规则也采用 X.500 格式。
- **证书持有者公钥（Subject public key）** 必选项。即主体的公钥和它的算法标识符。

- ❑ **证书颁发者唯一标识号（Issuer unique identifier）** 可选域。它含有颁发者的唯一标识符。
- ❑ **证书持有者唯一标识号（Subject unique identifier）** 可选域。证书拥有者的唯一标识符。
- ❑ **证书扩展部分（Extensions）** 证书扩展部分是 V3 版本在 RFC2459 中定义的，可供选择的标准和扩展包括证书颁发者的密钥标识、证书持有者密钥标识符、公钥用途、CRL 发布点、证书策略、证书持有者别名、证书颁发者别名和主体目录属性等。

12.1.3　公钥基础设施组件

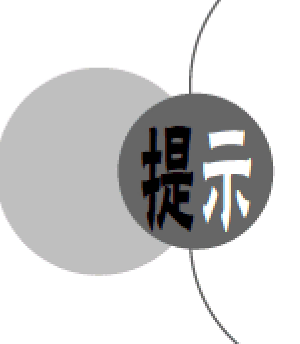
PKI 公钥基础设施是提供公钥加密和数字签名服务的系统或平台，目的是为了管理密钥和证书。一个机构通过采用 PKI 框架来管理密钥和证书可以建立一个安全的网络环境。通常公钥基础设置由多个组件构成。

1. 认证机构

认证机构是证书签发机构，它是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构。认证机构是一个实体，它有权利签发并撤销证书，对证书的真实性负责。在整个系统中，CA 由比它高一级的 CA 控制。

CA 负责确认身份和创建数字证书以建立一个身份和一对公/私密钥之间的联系。从某种角度来讲，它由这一过程中所使用到的软件和硬件组件及服务集合所构成。它还包括了人、操作过程和环境，以及规定如何确认身份和颁发什么格式的证书的策略。

CA 制定了一些规则，通过这些规则使申请者和证书用户确信该 CA 所确认的身份符合自己的目的并且是可以信赖的。而描述 CA 在各方面受到的约束情况及运作方式的规则都被定义在一个名为认证操作管理规范（Certification Practices Statement，CPS）的文件中。颁发证书的 CA 必须将它的认证操作管理规范提供给证书用户。如果一个 CA 没有 CPS，那么人们就会有理由怀疑该 CA 的真实性并降低对该 CA 所颁发身份的信任程度。



最初，CPS 是用来记录 CA 运作信息的，但最近人们越来越担心 CPS 实际上会泄露太多的信息。因此，目前人们正在讨论一个新的文件类型，并将其命名为 PKI 信息披露规范（PKI Disclosure Statement，PDS），它用来传达 PKI 操作所需的信息，例如，建立信息关系时需要的某个 CA 由另一个 CA 所证实这样的信息。

2. 注册机构

注册机构负责申请者的登记和初始鉴别。申请者是指那些提出登记请求并在请求批准后被授予证书的用户。这样的交互可能还包括证书撤销以及申请者在同 PKI 交互时需要的其他服务。RA 及其接口既可以被实现为证书服务器的一部分，也可以形成一个独立的组件。

RA 的职责可以由一个担任操作者的人来执行，所有的身份确认过程都可以被认为是一组

手工操作的过程（实际中，某些安全性要求较高的环境会要求直接由人来确认身份）。RA 职责就是将来自某个具有合法资格并且经过认证的用户的证书请求提交上去。

控制证书申请者登记和证书生成的业务规则多种多样，一个 CA 所用到的所有这种规则都应该在 CA 的 CPS 中描述。那些准备使用由该 CA 颁发的证书的企业中的安全管理员应该仔细查看 CPS 中所描述的各个方面的内容。

3. 证书服务器

证书服务器是负责根据注册过程中提供的信息生成证书的机器或者服务。用户的公钥，连同其他一些标识信息以及得到的证书结构一起用 CA 的私钥签名。

CPS 中管理证书服务器的部分包括了对如何确定 CA 密钥的安全，哪些信息将被放到证书当中，以及对撤销信息多久生成一次等问题进行描述。

4. 证书库

在投入使用之前，证书和相应的公钥需要对外公布。如果提供了某种公布机制以支持公开证书的分发，那么证书库通常是发布证书的地方。

通常用作证书库的目录可以是 X.500 的目录，但更为常见的是 LDAP 目录。LDAP 实际上是对用于在目录中定位信息的访问方法和协议的描述。一个 LDAP 兼容的目录可以实现为任何东西，从普通文件到关系数据库，甚至可以是一个 X.500 目录，但前提是它必须遵从 LDAP 的要求。



当由证书所有者发起到证书用户的连接时，证书也可能被直接分发给特定用户。

5. 证书验证

证书用户在收到证书时，需要对收到的证书进行验证，以确保证书的有效性、可信性以及是否符合自己的需求等。通常验证一个证书包括如下几个方面。

- 验证该证书的签名者的签名。
- 检查证书的有效期，确保该证书仍然有效。
- 检查该证书的预期用途是否符合 CA 在该证书中指定的所有策略限制。
- 确认该证书没有被 CA 撤销。

通常，验证证书链的过程非常复杂，特别是对于跨企业使用时尤其如此。证书链的验证可能在客户端计算机环境下执行，通常由使用该证书的应用程序完成。另外，也可能作为一种服务提供，客户端计算机可以使用该服务执行相同的任务。

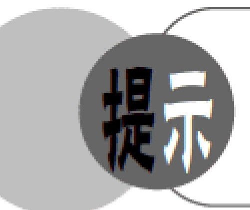
6. 密钥恢复服务

公/私密钥对可能是在本地的某个像 Web 浏览器这样的应用程序的密钥存储中生成，也可能是在某个像智能卡这样的物理设备上生成。另外，密钥对也可能是在某个集中的密钥产生服务器上被创建。

无论是哪一种情况生成的公/私密钥对，都需要有这样一种机制，即能够使得加密密钥被存档，并且如果它们被意外地丢失了也能够被恢复。除此之外，还存在一些其他情况，例如执法部门可能需要向当事人索要加密密钥。这种机制的存在使得即使密钥的持有者发生了什么不幸而导致公/私密钥对丢失，那么企业也可以通过使用密钥恢复服务来恢复这一至关重要的信息。

7. 时间服务器

可靠的时间，与数字签名一样，是发布可验证的时间戳所需要的前提条件之一。这需要一个单调增加的精确时间源，还需要对时间戳进行安全地传输以保证其不被窃听或者替换。最后，还需要对时间戳签名以便人们能够验证这个可信时间值的发布者是谁。



单调增加是指时钟（时间）一直向前走，这意味着无法将时间流重置为以前的某个时刻。

许多业务都会从可靠时间这一概念中获益。其中，包括可靠的审计日志、接收确认系统、工作流系统以及电子文件（包括电子合同）。为了得到一个可以在将来被认证的时间戳，用户通常需要一个以某种可信的方式提供的可靠的时间源，该时间源还应当具有单调性（时间必须一直向前走）。此外，还必须能够证明添加了时间戳的文件没有被修改过（需要用到数字签名）。

作为 PKI 的一部分，时间服务器会为分层的服务或者应用程序提供数字式时间戳。对于那些为像合同检验这样的应用程序提供支持的企业服务来说，其存在的价值取决于第三方对其使用时间戳的信任程度。在某些情况下，也需要使用一个可信的第三方时间戳提供者。

8. 签名服务器

数字签名通常是由那些应用了数字签名的事物处理或者管理文件的应用程序生成。如果该应用程序本身没有提供这样的支持，或者人们更希望使用一个集中的签名和验证服务，那么采用一个单独的服务器来专门为用户事物执行这一功能会是一个比较好的选择。签名服务器可能还会是构成像数字公证人所提供服务那样的第三方服务的基础。

12.1.4　授权的作用

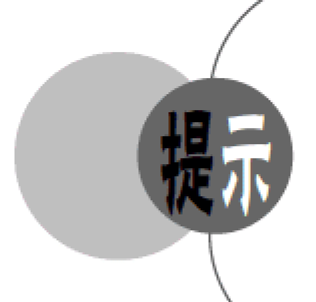
PKI 的首要任务就是确定可信赖的身份，这和确定该身份的持有者能够做什么事情不一样。在 PKI 中，关于允许一个合法用户对信息或者系统进行访问的决定一般是由授权系统而非认证系统作出的。

例如，作为一名合法的护照持有者，拥有一个由可信的 CA 证明的身份。当该用户为了进入一个不同的国家而走进该国的海关或者移民办事处时，对方会采用一套程序来检查护照的合法性。通常，对方会查看该用户的照片，并且可能让其在一份入关文件上签上手写的签名以便和护照上的签名进行对比。接着，对方会查看护照的全息图片，以核实它的确是用户所在国家的政府生成的，另外，还会核实其可识别的条形码当中的信息和护照中的物理信息

是否匹配以确定该文件没有被修改过。最后，会通过计算机调出用户的记录并检查该护照是否合法或者被撤销。这些步骤属于认证过程，它和证书用户检查证书的有效性所使用的步骤相似。在完成该过程后，对方就会知道该用户是否拥有一份合法身份并且也许会允许该用户进入该国。

另外，是否允许进入取决于该国是否具有某项安全政策规定必须拥有签证才准许入境。如果用户没有和该国想进行的访问类型相符的正确种类的签证，那么即使身份检验合格，也会被拒绝入境。

签证是一些额外信息，用于表明护照用户可能会希望利用的一些访问权限。护照确定用户的身份，而一份与护照相关联的签证则规定了用户可以做什么。



在该例中，用户的身份没有改变。证书颁发者和与其相关的信任级别也没有改变。对用户的身份验证过程也没有改变。所有这些都是确定用户身份所必须满足的先决条件。它们对应于认证系统（authentication system）。一旦认证完成，对方就有必要查看用户的护照，查看是否具有相应的签证。

在某些环境中，这也许是可以接受的，例如，证书可能是由一个企业颁发的，并且仅用于访问该企业内部的系统。在该企业内部，也许知道该用户的身份就足够了，因为它只不过是一张能让用户通过系统的普通通行证而已。

然而，随着 PKI 越来越多地被用来为不同企业间的交互或者企业与客户间的交换提供支持，除了认证之外，对授权的需求也变得越来越重要。

1. 证书和用户权利

在 X.509 中规定的数字证书使用唯一识别名来指定身份。而 X.500 命名方案构成了证书的主体和证书颁发者的唯一识别名的基础，它允许在证书中包含一些特定的信息从而实现基于角色的身份验证。例如，可以在一个命名方案中指明给一个用户颁发证书的证书颁发权威机构属于哪个公司的哪个部门，在此使用的唯一别名格式如下所示。

{Country=US，Organization=RSA Security，Organizational unit=Engineering，Location=Sweden}或者，证书的主体是一个人，他的名字指明了他的工作部门。

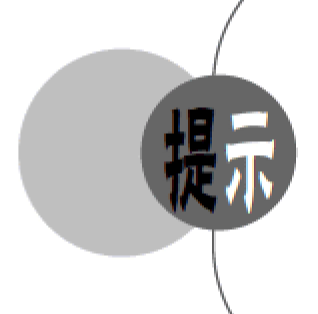
{Country=US，Organization=RSA Security，Organizational unit=Engineering，Location=lyl}

通过分析可信身份的名字，可以知道该用户能够访问的工作部门，如果证书颁发机构是瑞典工程组的 CA，那么就允许证书的所有组访问该工程组所使用的代码管理系统。这样，就可以创建一个按照功能和地理位置划分的授权系统。该授权系统依赖于分散在组织各处的 CA，这些 CA 不仅为组织中的特定人员确定身份，而且还可以批准对组织拥有系统的访问。

主体名字段中的唯一识别名并不是定义可用于授权目的属性的唯一渠道。其他证书字段也可以用于指定各种信息，如与证书颁发和使用控制相关的策略。另外，还可以将特定站点的信息编码到对证书的专用控制当中。

在 Microsoft Windows Server 2008 中，使用策略字段来指定证书持有者对系统的不同部分能够进行何种类型的访问。例如，一个使用智能卡的用户，可以利用保存在其上面的私钥进行签名操作。然而，如果该用户没有使用智能卡进行认证的附加权力，那么就无法使用该智

能卡登录到 Windows 桌面。另外，还可以使用其他策略标识来控制用户对 Windows Server 2008 应用程序的访问，或者指定用户对系统不同部分的管理功能。



一般来讲，将用于授权目的的信息存储在证书中会遇到这样的问题，即一个用户所拥有的角色或者权力要比其身份改变的更为频繁，CA 在运作上有开销，如果重新颁发证书给太多的用户，那么将有更大的代价。一般证书有效期大约是 1 年或者 2 年，如果要处理不断变化的用户访问权限的话，该有效期必须以天或者小时来计算。

2. 特权管理基础设置

在过去的几年中，对用户能力和特权的管理已经吸引了许多人的注意力。许多授权系统纷纷出现，但是几乎所有的这些系统的实现都是专有方案。每种解决方案在开发中涉及的受管理用户属性种类、基础设置的工作机制、使用的信任模型等内容都各不相同。

为创建能够在各厂商之间或者是不同企业间共享的方案，人们制定了 PMI（特权管理基础设施）作为支持授权系统的基础设置，PMI 和支持认证系统的 PKI 之间具有非常紧密的联系。

PMI 的基础单元或者结构是一种被称为属性证书（Attribute Certificate，AC）的新型证书，这种类型的证书有时候也称为特权属性证书（Privilege Attribute Certificate，PAC）。与 PKI 中对应的身份证书不同，PMI 属性证书并不会创建身份并将该身份联系到某个公/私密钥对上。它们所做的是对一组与用户相关的属性进行编码，且这些属性并不局限于访问权限或者特权。

12.2 PKI 服务和实现

随着网络应用技术的发展，安全隐患也越来越多，尤其是在一些未经允许授权用户访问的网络，一旦数据被人截取、篡改或假冒，都会给企业和用户带来难以想象的损失。因此，安全问题也越来越被人们重视，特别是电子交易类网站。而通过 PKI 服务能够有效地提高通信的安全性以及实现用户的身份认证、数据加密等功能，从而保护用户的网络及传输信息的安全。

12.2.1 密钥和证书的生命周期管理

密钥和证书生命周期管理涉及对密钥和证书从创建到撤销的整个过程。最初，需要创建公私密钥对，并且将它们关联到用于确定某个最终实体身份的证书上。作为向 CA 注册和申请证书过程中的一部分，该密钥对连同其他一些标识信息一起被提交给 CA。CA 在核实身份信息之后，就会颁发该证书。

在证书可以用来验证身份之前，必须通过各种各样的方式将证书分发给证书用户。证书可以由证书所有者发送给证书用户，也可以由 CA 保存在某个证书库中供用户索取。

但是，颁发给用户的证书的生命期限是有限的。如果到了截止日期，该证书就会过去，此时必须重新颁发一个新的证书。在为某个特定的身份重新颁发证书的过程中，证书的某些信息可能会发生变动。或者，因为密钥有一个平均使用寿命（取决于密钥的长度），所以证书和密钥必须定期更新。

发布一个最终实体证书的 CA 可能需要作废该证书。在这种情况下，该证书应该被撤销，同时，该 CA 需要公布这一撤销消息。

另外，由于密钥可能会丢失并且可能需要恢复该密钥以解密以前用它加密的信息。所以需要密钥归档和密钥恢复的机制。

12.2.2 密钥管理

密钥管理确保了专用密钥的安全存储和保护，这是实现 PKI 的安全性所必需的。如果非密钥实际持有者的其他人能够使用专用密钥，则 PKI 安全模式将受到破坏。因此，在一个 PKI 环境中，特别是在一个对于商务流程、财务往来或访问控制而言至关重要的 PKI 环境中，必须通过可靠的密钥管理解决方案来对专用密钥进行保护。

1. 密钥生成

密钥对的产生是证书申请过程中重要的一步，其中产生的私钥由用户保留，公钥和其他信息则交由 CA 中心进行签名，从而产生证书。根据证书类型和应用的不同，密钥对的产生也有不同的形式和方法。对普通证书和测试证书，一般由浏览器或固定的终端应用来产生，这样产生的密钥强度较小，不适合应用于比较重要的安全网络交易。而对于比较重要的证书，如商家证书和服务器证书等，密钥对一般由专用应用程序或 CA 中心直接产生，这样产生的密钥强度大，适合于重要的应用场合。

另外，不仅要生成好的公/私密钥对，而且要保证它们的安全。好密钥通常具有不易猜测、具有足够的长度等优点，且应该只让适当的人知道。一般采用非对称密钥机制，它在系统的服务端和用户端分别生成自己的密钥对，然后互传公钥，并保存各自的私钥，使用公钥实现消息的加密和对签名的认证，用私钥实现解密和签名。

在开始创建一个密钥生成系统时，需要考虑许多安全事项，因为这些实现可能会影响用户对集中式或分布式密钥生成系统的选择。例如，支持硬件随机数发生器的高性能中心处理单元的有效性以及密钥生成的单一验证实现，可能导致用户选择一个中心密钥产生服务。但是，中心密钥生成方案也会带来一些问题，例如，密钥安全传输到用户以及确保用户有足够的安全措施来防止由于操作管理而破坏密钥发生器的输出等。另外，一些客户可能没有准备好接受外部所产生的密钥，即使该密钥的产生和管理是安全的。

中心密钥使得密钥归档和恢复之类的服务简单化，因为只有少量的基础设施组件对归档系统有接口。这在大多数情况下运行得很好，因为加密密钥是最有可能都需要保存在归档系统中的密钥类型。在本地生成的数字签名密钥几乎从来不需要归档。

2. 密钥归档和恢复

在单位或公司网络中，常常会发生用户忘记自己的口令等麻烦事情，而要求管理员给他

们访问他们账户的新口令，这无疑增加了管理员的工作负担。同样，在 PKI 中也可能发生数据加密密钥的丢失。因此，为了保证系统的安全性，大多数组织都会增加使用密钥归档和恢复系统功能，允许用户重新获得丢失的密钥。

如果用户的私钥丢失或无法访问，就会导致无法恢复使用此密钥加密的信息，而且有时必须恢复一个旧的私钥来解密一个加密文件，如邮件系统在某天使用了新密钥，但如果想阅读当天以前的加密邮件，就必须使用旧密钥。

密钥归档系统主要与密钥备份库或者档案中的密钥安全存储有关，而密钥恢复系统主要与恢复密钥的操作有关。当然，两个系统和它们相应的机制紧密相连，但是考虑组织安全策略和设计约束，通常将它们作为独立系统保存。

PKI 系统拥有完成密钥的存档和恢复的功能。它能够维护每个用户的密钥记录，而且能够在必要时从这个记录中恢复密钥，控制用户私钥的备份与恢复。

另外，密钥应该是以一种不易受到攻击、加密的形式存储在一个机构中，但由于用户在不同阶段会使用不同的密钥对（如每年更新密钥对），所以密钥的备份变得很复杂。为了实际需要，需要随时保存先前的密钥，并且它们要像当前密钥一样是可访问的，需要保存的时间至少是 12 个月。对于旧密钥（比先前更早的密钥），应该可以从离线的存储档案中获得恢复。

对密钥档案的访问需要严格的控制，通常这个系统的安全至少和中心密钥产生系统一样敏感。虽然密钥产生系统可能在创建密钥时受到复制密钥的攻击，密钥档案包含 CA 注册过程中已经证明的所有密钥。在抗篡改安全硬件模块中可能需要保护密钥。访问系统可能要求几个管理员同时在场，以减少存储密钥潜在的欺骗或者偷窃等安全隐患。

12.2.3　证书管理

证书管理用来处理在证书生命周期内应用于证书操作的集合。在完成注册过程之后，CA 必须对证书负责。

1. 证书发放

通过注册中心的初始身份认证后，注册中心将用户的申请提交到认证中心，认证中心根据证书操作管理规范定义的颁发规则在证书中插入附加信息并设置多个字段。例如，注册机构和认证策略可能需要颁发不同种类的证书，代颁发的身份类型不同，证书中心的策略设置也会有所不同，以此限制证书的使用方式，证书生成后根据 CA 实现方式的不同以及认证操作规范需求的不同将证书返回给用户（如以电子邮件形式返回）。

2. 证书更新

根据颁发证书的不同类型，证书更新也包括以下几种不同类型。

❑ **最终实体证书更新**

如果与证书相关的密钥可能已经达到它的有效生命终点，或证书可能已过期（与签署的有效期比较），或者证书中的某些属性已经发生改变，并且对于这些新的属性必须重新证明，这时就需要发放新证书。但只要证书没有被撤销，那么之前的密钥和证书就能用来完成认证过程。

❑ **CA 证书更新**

CA 要对所颁发的数字证书和撤销的数字证书使用私钥签名，这个密钥可能过期，或者 CA 本身的证书中有些属性可能要修改。另外，由于 CA 证书一般由上级 CA 颁发，这同样有一个有效期的问题。因此要对 CA 证书进行更新。

从概念上来讲，CA 密钥对的更新与最终实体密钥对的更新类似。然而由于依赖根 CA 的团体的数量，可以采取一些方法使得向新密钥和相应 CA 证书的转换更顺利。PKIX 使用 CMP 规范中的根 CA 确认一个模型，这个过程对根 CA 起作用，就像它们可以发行自签名的证书。这个过程依赖于 CA，使用它先前的密钥签名新证书，并且使用新密钥签名旧证书。这样的结果使得根 CA 经历一次密钥更新创建了如下 4 个证书。

- **旧用旧证书**　原始自签名证书，此时先前的 CA 私钥被用来签名 CA 证书中先前的公开密钥。
- **旧用新证书**　用新 CA 私钥签名的 CA 证书中的原始公开密钥。
- **新用旧证书**　用先前的 CA 私钥签名的 CA 证书中的新的公开密钥。
- **新用新证书**　用新的 CA 私钥签名的 CA 证书中的新的公开密钥。

先前的 CA 证书在密钥更新事件发生时由所有依赖方拥有。新用旧证书允许新产生的 CA 公开密钥由先前的、可信的密钥证实。一旦新密钥是可信的，依赖方获得的新 CA 证书将能够信任它，此时旧用旧证书和新用旧证书对于依赖方不再是必需的。新用旧证书的有效期限从新 CA 密钥的密钥产生时间开始，在所有依赖方转移到承认新密钥的适当日期结束。最后的可能时间是先前密钥的过期期限。旧用新证书实现旧密钥对向新密钥对的平滑转换，其有效期从先前的密钥对产生的日期开始，到旧证书过期的日期结束。在 CA 新旧证书交迭时期，旧证书和新证书都可以使用。

3. 证书注销

在某些情况下，证书的有效性要求在证书结束日期之前终止或者要求用户身份与私钥分离，证书要撤销，如签署者状态发生改变，证书中的信息可能已经修改，与用户相关的私钥可能以某种方式泄露。为了处理这类事件，必须要有一种方法来使这些证书无效。

注销证书可以由私钥拥有者（证书主体）通知 CA 或者由某个授权的个人提出，证书主体向 CA 提出证书注销要求时，必须提供撤销的确切日期。但是，证书的主体可能想逃脱责任，想要使以前签署的合同无效，它可能会提供签署日期之前的时间作为撤销日期。因此，这可能需要使用一个公证服务，它成为特定日期正确签名的证据。

如果证书颁发与用户管理系统相关联，用户记录的删除将产生证书注销通知，CA 就必须采取行动，撤销用户证书或使它无效，并警告证书使用者，该证书不再代表一个可信身份。在大多数情况下，CA 用来公布已经更改的证书状态机制是一个证书注销列表（CRL）。证书注销列表包括已被撤销证书的序列号与撤销日期，还有标志撤销原因的状态。CRL 由可信撤销服务的私钥进行签名，以保证列表不能被修改。如果把已撤销证书的条目从 CRL 中删除，会使证书注销过程无效；如果向 CRL 添加未被撤销的证书条目，则该证书本应正常服务却被废止，这会使拒绝服务攻击成为可能。CRL 也标识了它公布的日期以及在什么时候会出现下一个版本，以确保所使用的是最新的 CRL。CRL 通常公布在一个目录中，在证书验证时可以参考。证书用户在验证证书的同时也可以从目录中下载 CRL，并查询列表寻找被验证的证书

序列号。

CRL 的公布周期由 CA 决定。公布的时间间隔可以是一天或者一星期，这依赖于认证操作规范（CPS）定义的策略，如证书用户正在处理高价值的金融事务，则可能希望一小时或者更短的时间公布一次通知。CRL 更新的频率对证书使用者可以寄予多高的信任级别有直接关系。如果 CRL 刚刚公布，之后马上有一个证书被撤销，则在下次 CRL 公布时，撤销状态才能到达使用该证书的用户，这可能需要经历相当长的时间延迟。证书验证者可能需要更多的最新信息，而不仅仅是特定 CA 所提供的信息。如果使用来自多个 CA 的证书，可能要考虑 CRL 公布间隔的不同。此外，定位 CRL 存储的目录，下载 CRL 并处理其中的内容，可能需要相当多的最新信息。

另外，也可以使用撤销机制挂起证书，使证书处于临时冻结状态，这种机制适用于证书拥有者确定在一段时间内不会频繁的使用证书，并且想确保在这段时间内证书不被使用。证书的状态不明确时，也可考虑使用证书冻结。当过一段时间后，证书被证实确实应该撤销时，将在下次公布的 CRL 列表中删除，并且需要时可经过处理后再次被用作有效证书。

4. 证书验证

证书验证是确定证书在某一时刻是否有效以及确认它能否符合用户意图的过程。它包括以下内容。

- 证书是否包含一个有效的数字签名，以确定证书内容没有被修改过，保证数据的完整性。
- 当前使用证书的时间是否在证书的有效期内，或在证书签发时的起止日期内。
- 证书是否用于最初分发它的目的。
- 检查证书注销列表 CRL，验证证书是否被撤销。

12.3 PKI 的体系结构

公钥基础设施就是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证信息的机密性，又保证信息具有不可抵赖性。到目前为止，它是公认的保障网络社会的最佳体系结构。

12.3.1 公钥基础设施体系结构

在 PKI 中包括多种组件，通过这些组件能够构建一个安全的网络环境。在构建安全网络环境的过程中，如何将各种组件和服务结合在一起，以及使用哪一种体系结构是很重要的，而 PKIX（标准的公共密钥基础结构）则规定了各种组件间的相互作用。

1. PKIX 模型

X.509 标准规定了证书的格式和应用范围，以及公开密钥分配的过程。作为一个重要标准，

需要包含许多使用领域，允许证书内容有许多变化，并支持许多可能的操作模型。

公开密钥基础设施 X.509（Public Key Infrastructure X.509，PKIX）工作组由 Internet 工程任务组（IETF）组成，主要用来规定证书概要文件集合和操作模型，适用于在 Internet 上部署 X.509 公开密钥。它已经为不同的应用领域创建了其他 PKI 模型，例如 ANSI ASC C9F 为金融机构开发的标准。每个模型根据需要选择 X.509 属性，并且可以增加证书扩展或者概念以支持不同应用领域的需要。

在 PKIX 中定义了注册、初始化、认证、密钥对恢复、密钥产生、密钥更新、交叉证书、撤销、证书和撤销通知的分发/发布等大部分公钥基础设施功能。为支持它的体系结构模型，PKIX 撰写了专门文档来描述如下 5 个领域。

- X.509 V3 证书和 V2 证书撤销列表概要文件。
- 操作协议。
- 管理协议。
- 策略概要。
- 时间戳和日期认证服务。

这些方面提供了几种方式来细化基本的 X.509 描述。概要文件提供的 X.509 子集包括那些被认为对 Internet 组织有用的扩展。另外，对于不同环境下的因特网操作，扩展可以被标识为关键的或者可选的。

操作和管理协议用来描述 PKIX 兼容组件为了彼此互操作而必须支持的信息。与操作协议不同的是，在管理协议上将花费更多的注意力。因为操作协议利用现有的 Internet 协议来提供服务，如 FTP 或 HTTP，并且在大多数情况下确定应该如何使用这些协议来支持 PKIX 模型，因此比管理协议简单。

策略概要描述应该如何使用证书或者应该如何操作 PKI 组件。大多数情况下，应该提供文件来控制 PKI 操作，概要是 PKI 执行关于这些文件种类的指示或指南。而时间戳和日期认证服务与其他领域不同，它包括描述分层或辅助服务的文档，在创建安全服务时 PKI 实现可能要求分层或辅助服务。

2. PKIX 体系结构

PKIX 体系结构内的主要组件包括如下几个方面。

- **客户**　包括 PKI 证书用户，否则被确定为最终实体和最终用户或系统（PKI 证书的主体）。
- **证书机构**　主要用于发行和撤销 PKI 证书。
- **注册机构**　用于确定公开密钥和证书持有者身份之间的连接。
- **资料库**　用于存储证书和 CRL 的系数（可能是分布式的）以及向最终实体提供证书和 CRL 的分发机制。

图 12-2 所示为 PKI 组件及其相互间的主要关系示意图。在图 12-2 中操作事务、管理事务及证书和 CRL 公布属于 PKIX 组件之间的工作流。其中，操作事务是包含在操作协议文档中的消息交换，提供证书、CRL 和其他管理与状态信息的优先传输；管理事务是管理协议文档中描述的消息交换，它提供通知服务，支持 PKI 内的管理事务或操作；公布用于向公开库分发证书和 CRL。



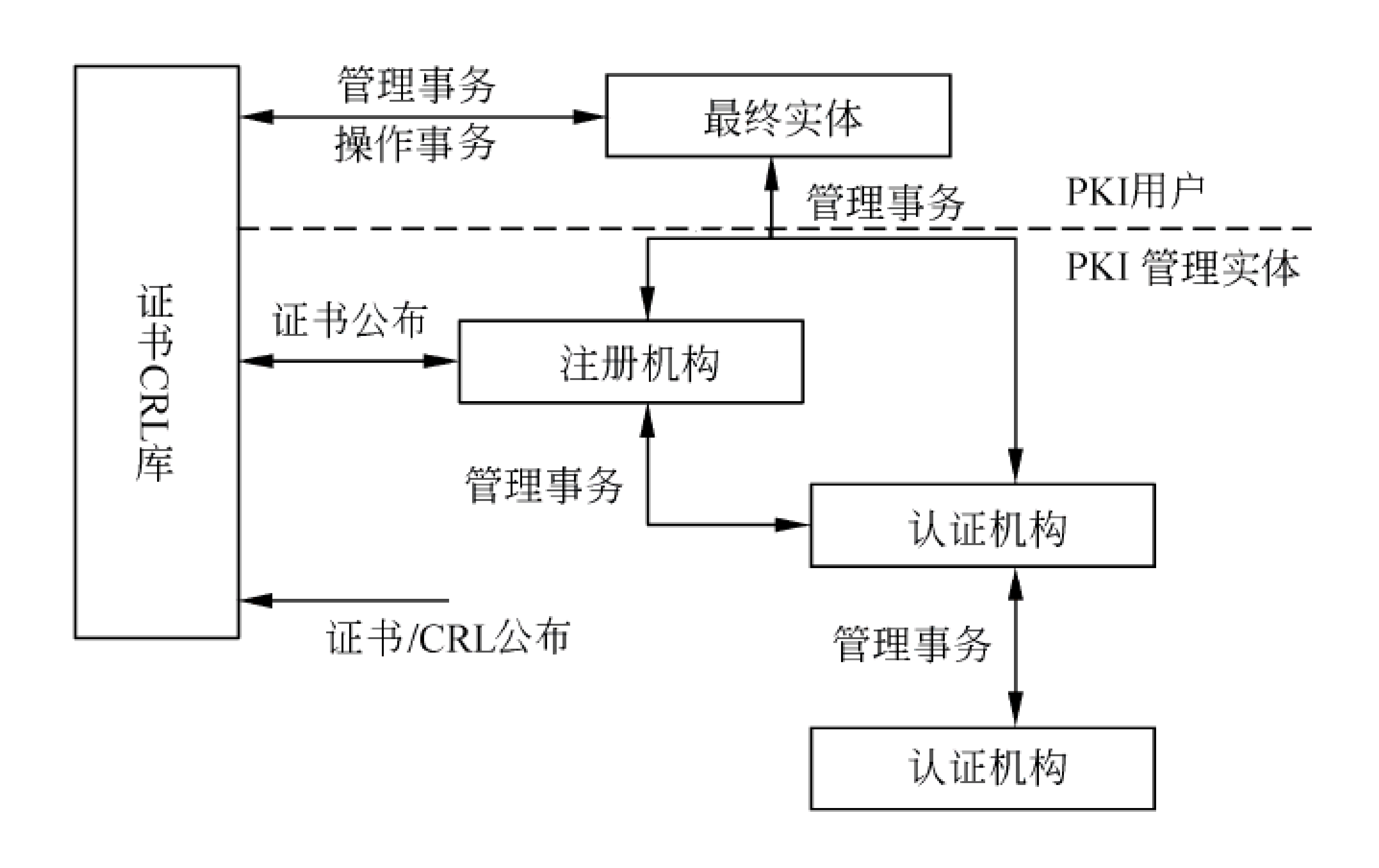


图 12-2　PKI 组件

12.3.2　PKI 实体

PKI 最主要的任务就是确定可信赖的数字身份，接受 PKI 服务的用户都确信自己没有被误导和欺骗。创建可信赖的身份问题就是要找到通信各方都完全信任的人或机构来证实对方的身份，如果能找到一个合适的人或者实体，而这个人或实体能够有相当大的把握认定他所采用的证实创建身份准确性的处理是正确有效的，它所提供的身份证明机制也是合理且不可伪造的，那么用户就可以在某种程度上信任他所创建的名字或身份。

通常一些特定的权威机构具有证实身份的权力或者能力，如公安局可以颁发身份证，护照管理局可以提供护照等，而且也需要有多种权威机构提供不同用途的证件来实现不同的用途，通常这些机构就是实施 PKI 服务的实体。

实施 PKI 服务的实体概括起来分为注册机构、认证机构和证书库 3 个部分。其中，注册机构是 PKI 实体的核心，是 PKI 服务的提供者；认证机构是 PKI 的用户，是 PKI 服务的使用者；证书库是一个分布式数据库，用于证书或证书注销列表的存放和检索。

1. 注册机构

注册机构是 PKI 内部的可选实体，它负责与注册最终实体（CA 发行的证书的主体）相关的管理任务。如果 PKI 中没有 RA，则认为 CA 与注册机构规定的性能有相同的性能集合。

特殊注册机构实现的功能通常随着 PKI 实施的需求而变化，但是必须支持确定或者确认签署身份者的原则。这些功能可能包括如下几个方面。

- 主体注册证书的个人认证。
- 确认主体提供信息的有效性。
- 通过被请求证书的属性来确定主体的权利。
- 确认主体确实拥有注册的私钥（一般称为拥有凭据 POP）。
- 在需要撤销时报告密钥泄露后终止事件。
- 为识别身份的目的分配名字。

- ❑ 在注册初始化和证书获得期间产生共享密钥。
- ❑ 产生公/私密钥对。
- ❑ 认证机构代表主体最终实体开始注册过程。
- ❑ 私钥归档。
- ❑ 开始密钥恢复处理。
- ❑ 包含私钥的物理令牌（智能卡）的分发。

一般来讲，注册机构控制注册、证书传递、其他密钥和证书生命周期管理过程中主体最终实体和 PKI 间的交换。然而，任何环境下 RA 都不真正发起关于主体的可信声明。因此，只有证书机构可以颁发证书或者颁发证书撤销状态信息，如 CRL（证书吊销列表）。

单个注册机构的部署是与 PKI 操作相关的商业处理的重点。例如，在管理 PKI 服务中，可能在一个站点执行 RA 的操作，同时 CA 和它的操作可能是外购的。因此，选择证书发行可以在组织内部维护，同时处理可以分配给用户的商业伙伴或者作为特区进行操作。

另外，在某些情况下，可能要求认证机构管理网络外部的最终实体访问注册机构服务器。如图 12-3 所示，当使用证书来认证用户的商业系统时，用户的外部网络环境下的伙伴组织内的最终实体的注册。在这种情况下，RA 可以放置在网络的 DMZ（隔离区）中，但是为了保护 CA，需将它放在网络防火墙的后面进行维护。

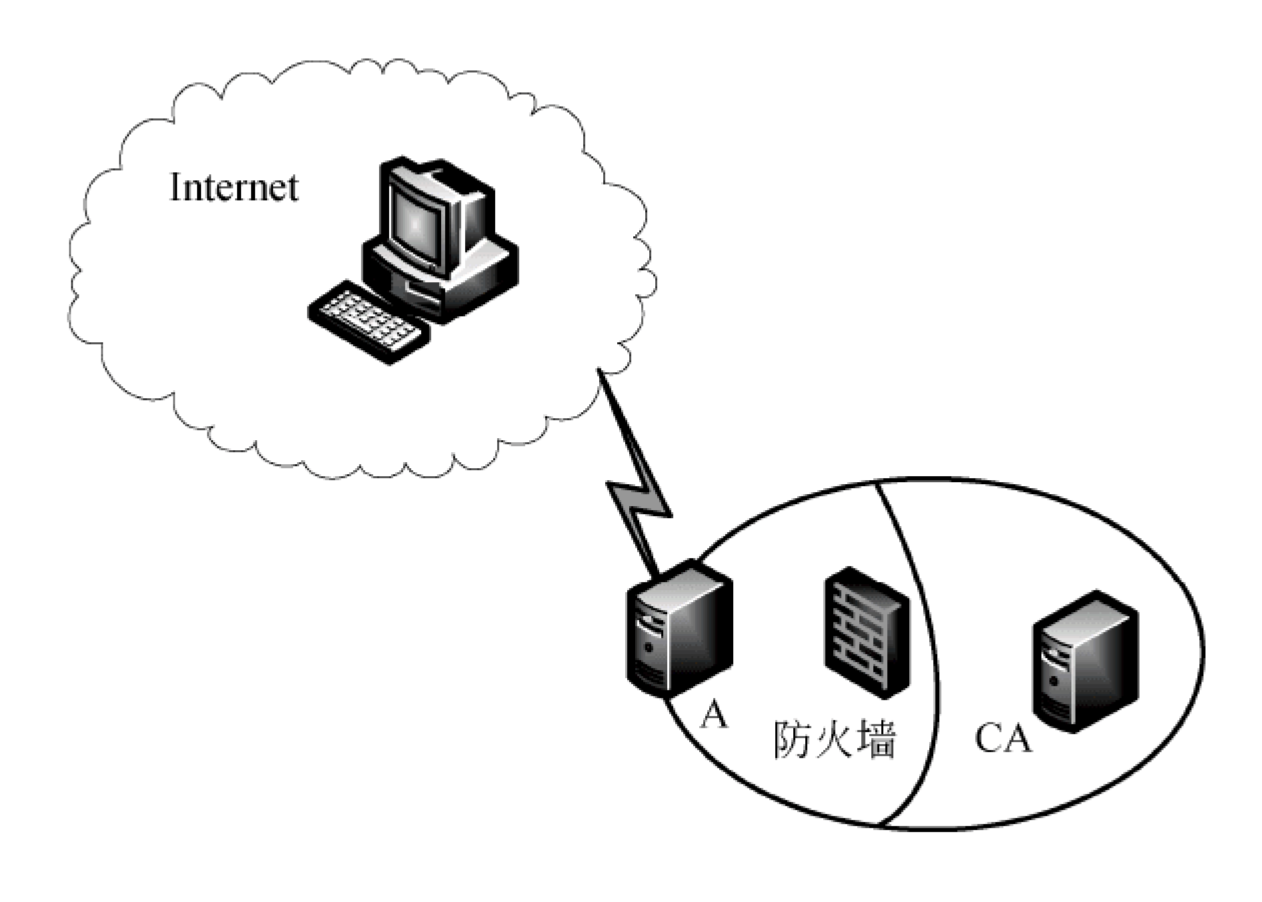


图 12-3　访问网络 DMZ 中的注册机构

2. 认证机构

认证机构负责创建和发行最终实体证书。最终实体证书将主体最终实体的身份表示成正在注册的主体名字，注册使用与主体拥有的私钥相应的公开密钥。

另外，CA 负责在证书发行之后对证书生命周期所有方面的管理，这包括跟踪证书状态，并且在证书需要撤销时发行撤销通知。即使有撤销通知的服务，CA 仍然需要维护证书档案和与证书相关的审计，以满足日后验证的需要。

在 PKIX 中，存在大量与特殊类型 CA 相关的特殊术语。例如，根 CA 是一个直接被证书用户信任的 CA。但在 PKIX 中，并不一定使用该术语，如它使用“可信锚”来称呼被证书用户信任的 CA。

3. 证书库

证书库被用作证书和 CRL（证书吊销列表）的公共存储。最初，证书库是一个 X.500 目录。但为了支持 PKIX，证书库通常是一个 LDAP 目录。

LDAP 作为 PKIX 明确支持的一个操作协议被列出。虽然像 CMP 之类的管理协议内的操作，即为了获得特定证书或者 CRL 可能提供的查询支持，但是 LDAP 可以直接用作这些相同信息的查找协议。

另外，证书库除存储证书和 CRL 外，还可能使用目录中的其他实体（如 CA 目录客体）来存储附加信息（包括身份确认关系）。

不同的实体间通过 PKI 操作完成证书的请求、确认、发布、撤销、更新和获取等过程。PKI 操作分为存取操作和管理操作两类。前者涉及注册机构、认证机构与证书库之间的交换，操作的目的是向证书库存放证书和 CRL，或从证书库中读取证书和 CRL；后者涉及注册机构与认证机构之间或注册机构内部的交互，操作的目的是完成证书的各项管理任务和建立证书链。

12.3.3　PKIX 证书验证

为了将 X.509 标准应用到 Internet 上，建设基于 X.509 标准的 PKI 系统，IETF（Internet Engineering Task Force）在 1995 年成立了 PKIX 工作组，开始制定各种与 Internet 相关的 PKI 标准。

由于 X.509 标准的重要基础就是 PKIX 工作组，因此，在 PKIX 的系统结构中，也包括了类似的 CA、末端实体（证书持有者和依赖方）、CRL Issuer 和资料库。但不同的是，X.509 标准中描述的资料库是指 X.500 目录；而 PKIX 系统结构的资料库，除 X.500 目录外，还可以使用各种常见的 Internet 信息发布技术，包括 LDAP 协议、HTTP 协议、FTP 协议等。PKIX 工作组还制定了使用 LDAP 协议、HTTP 协议、FTP 协议从资料库获取证书和 CRL 的相关标准。

PKIX 系统结构中，还包括了 RA 和 OCSP 服务器。RA 承担了 CA 委托的一部分证书管理功能，是 CA 与用户之间的通信接口。OCSP 服务器是由 PKIX 工作组提出的。证书验证者使用 OCSP 协议与服务器在线通信，可以更加及时地获得证书的撤销状态。

另外，PKIX 工作组还定义了证书申请、撤销、更新等各种操作时，末端实体与 RA、CA 之间的通信格式。当 RA、CA 相互通信时，它们也使用证书来保证安全，此时 RA、CA 也具有证书持有者和证书验证者的功能。

1. OCSP

在 RFC 2560 中定义了在线证书状态协议（Online Certificate Status Protocol，OCSP），主要是为了克服基于 CRL 的撤销方案的局限性，并且为证书状态查询提供即时响应。即返回特定证书撤销通知，而不是使用 CRL 形式的大量线性搜索列表。

❑ **OCSP 操作**

OCSP 是一个简单的请求/响应协议，可基于多种协议传输，但最经常使用的是 HTTP 协议。OCSP 使用证书序列号、结合发行 CA 名称和公开密钥的散列值，确认作为查询目标的证

书。其中，被称为 OCSP 响应程序的服务返回证书状态。响应通常返回值正常的、已撤销的和未知的 3 种状态来指明证书状态。

另外，返回的大量“活跃度”标识，表明了响应信息的及时性。通常包括 thisupdate（指定状态正确的时间）、nextupdate（比较新的状态信息可用时的时间）和 producedAt（OCSP 响应者对请求签名的时间）3 个方面。

OCSP 的工作方式存在大量的内在限制。仅仅在单一证书上返回信息，没有验证与证书相关链接的有效性，依赖方软件必须执行证书链或路径处理所要求的其余工作。例如，在验证最终实体之前，依赖方必须下载发行最终实体证书的 CA 证书。为了计算最终实体证书状态请求要求的散列值，需要颁发者的公开密钥。

OCSP 响应程序不提供认证路径结构。构造路径相关证书的位置留给依赖方处理。另外，它也不发送给 OCSP 响应者的完全证书，相反，为了验证所需要发送信息给 OCSP 响应程序，如证书序列号，因此，不可能验证证书中的签名。由于 OCSP 仅仅与证书的撤销状态有关，因此，客户必须检查其他验证信息，如证书有效期、密钥使用一致性以及其他约束。

❑ **功能选项**

为了检查证书集合的当前有效性或者有可能使用 CA 公布的现有 CRL，可以将 OCSP 响应程序配置成可以直接访问证书数据库。依靠策略要求执行证书有效性检查时，“新鲜性”标识为客户提供了可以使用的特定信息。在某些情况下，为了实现 OCSP，使用 CRL 引起的延迟可能不太重要，因此，可以不用查找目录、下载整个 CRL 或不用处理它所带来的方便性。

有些应用可能对 CRL 公布间隔并不敏感，如签署者服务，用具体例子说明或终止一个用户花费的时间可能提上议事日程。在这种情况下，在线服务以及简单消息接口的方便性使 OCSP 成为理想的解决方案。而 OCSP 响应程序数据库的正常 CRL 更新在后台发生的事实，在该例中是不相关的。

为了达到最优化，预先产生证书验证响应对实现是有效的。这就允许在后台对响应进行签名和存储，此时签名操作可以执行的频率限制了实现的响应时间。

另外，OCSP 允许委托证书验证，从而不必在证书服务器上实现 OCSP 响应。这允许更大规模的实现，同时与证书验证系统分离保存 CA 签名密钥。

2. SCVP

简单证书验证协议（Simple Certificate Validation Protocol，SCVP）的出现是为了克服 OCSP 协议存在的缺点。

SCVP 保留不可信和可信服务器的功能。例如，不可信服务器可以提供路径来构造所需要的中介证书，因此在这种情况下基于客户的认证路径验证的标准过程是足够安全的。可信服务器可以为依赖方执行全部验证服务。可信服务器的目标是消除客户端软件的路径验证开销，并允许执行中心验证策略。

SCVP 使用简单请求响应协议，设计目标超过了 HTTP 或 E-mail 的限度。对所有的 SCVP 响应程序签名。如果要求客户认证，或者为了不可否认性将请求计入日志作为审计踪迹的一部分，也可以对请求签名。

SCVP 与 OCSP 的主要区别是 SCVP 客户在将要验证的询问中发送证书集合，而 OCSP 可以发送证书标识。结果证书可以执行更多的验证步骤。客户可以发送中介证书的集合，SCVP

服务器可以将中介证书看作是验证处理的一部分，由客户来确定哪个根是可信的。在验证处理期间 SCVP 必须使用这些证书。

客户对请求可能指定的其他约束包括被执行的检查类型、考虑撤销消息的类型以及证书验证必须使用的策略，可以指定应该只检查撤销状态还是应该执行全部路径验证处理。撤销信息的类型允许客户指明，应该使用 CRL 或 OCSP 服务来获得证书的撤销状态。

客户可以确定服务器返回什么类型的信息及请求返回撤销状态数据，或者为了客户的进一步处理而返回用来验证证书的证书链。

SCVP 客户也可以请求在特定点上及时验证证书。这可以在验证签名时使用，例如，验证基于当时证书状态产生的签名当时是否有效等。

SCVP 并不像其名称所暗示的那么简单，它允许一定程度的证书验证的灵活性，并且允许中心服务器降低最终实体相当大的处理开销。然而，为了决定证书状态是否可信，必须向服务器传输数量可观的信息。

3. OCSP-X

如果 SCVP 依赖现有的机制，如 CRL 或 OCSP，并且证书状态检查和它的处理非常紧密，则认为扩展 OCSP 可能是一个更好的验证方案。因此，OCSP-X 被提议为 IETF 标准过程的一部分。

设计 OCSP-X 的目标与 SCVP 的目标类似，但是在 RFC 中对 OCSP-X 做出了更有效的规定。它所支持的附加功能包括在用于认证的特权管理机构中所使用的证书属性的验证。

在 OCSP 中，如果用户为了做出关于证书的可信决定而向服务器委托责任，那么客户可以不必重复信任过程。因此不需要向客户返回信息（如在该过程中实际验证的证书链或者使用的相关 CRL）。

与 OCSP 请求相比，在 OCSP-X 请求中增加了如下扩展字段。

- **指定可信根（Specify Trusted Root）** 该字段允许客户使用指定的根 CA 证书作为可信根来查询证书的有效性。如果服务器不能创建从最终实体到根的可信路径，则返回错误信息。
- **指定处理规则（Specify Processing Rules）** 该字段允许客户确定认证路径验证期间应该使用的处理规则。
- **评估可信路径（Evaluate Trust Path）** 该字段要求 OCSP-X 服务器创建一个来自可信根的路径，并随意返回创建或验证证书链所使用的部分或全部数据。
- **注册可信路径（Register Trust Path）** 该字段允许客户向服务器指明，指定的可选路径在某些特定时段是有用的。这样可以使服务器处于优化的目的缓存与可信赖路径有关的信息。

12.4　权限管理基础设施 PMI 概况

权限管理基础设置（Privilege Management Infrastructure，PMI）又称为属性特权机构，在 ANSI（美国国家标准学会）和 IETF（互联网工程任务组）的 PKIX 中都有定义，它依赖于公

共密钥基础设施 PKI 的支持，主要提供访问控制和特权管理，提供用户身份到应用授权的映射功能，实现与实际应用处理模式相对应的、与具体应用系统和管理无关的访问控制机制，并能极大地简化应用中访问控制和权限管理系统的开发与维护。

在国际电信联盟电信标准化部（ITU-T）2001 年发表的第四版 X.509 标准中，首次将权限管理基础设施的证书完全标准化。X.509 的早期版本侧重于公钥基础设施的证书标准化。

PMI 授权技术的基本思想是以资源管理为核心，将对资源的访问控制权统一交由授权机构去管理，即由资源的所有者来进行访问控制管理。与 PKI 相比，两者的主要区别在于 PKI 证明用户是谁，并将用户的身份信息保存在用户的公钥证书中；而 PMI 则证明这个用户有什么权限、什么属性、能干什么，并将用户的属性信息保存在属性证书（又称管理证书）中。

PMI 系统主要包括授权管理中心（AA 中心）和资源管理中心（RM 中心）两部分。其中，授权管理中心的主要设备是授权服务平台，它是实现 PMI 授权技术的核心部件，主要为用户颁发 AC 授权证书。

PMI 使用了属性证书（Attribute Certificate），它是一种轻量级的数字证书，这种数字证书不包含公钥信息，只包含证书所有人 ID、发行证书 ID、签名算法、有效期、属性等信息。一般的属性证书的有效期均比较短，这样可以避免公钥证书在处理 CRL 时的问题。如果属性证书的有效期很短，到了有效期的日期，证书将会自动失效，从而避免了公钥证书在撤销时的种种弊端。属性一般由属性类别和属性值组成，也可以是多个属性类别和属性值的组合。这种证书利用属性来定义每个证书持有者的权限、角色等信息。从而可以解决 PKI 中所面临的问题，对信任进行一定程度的管理。

1. PMI 模型

绝大多数的访问控制应用都能抽象成一般的权限管理模型，包括对象、权限声称者（privilege asserter）和权限验证者（privilege verifier）3 个实体。其中，对象可以是被保护的资源，例如，在一个访问控制应用中，受保护资源就是对象；权限声明者也就是访问者，是持有特定权限并声明其权限具有特定使用内容的实体；权限验证者对访问动作进行验证和决策，是制定决策的实体，决定被声明的权限对于使用内容来说是否充分。

通常情况下，权限验证者根据以下 4 个条件来决定访问通过或失败。

- 权限声明者的权限。
- 适当的权限策略。
- 当前环境变量（如果存在）。
- 对象的敏感度（如果存在）。

在这 4 个条件中，权限策略说明了对于给定敏感度服务的对象方法或权限的用法和内容，用户持有的权限需要满足什么条件及达到什么要求。权限策略准确定义了什么时候权限验证者应该确定一套已存在的权限是“充分的”，以便许可（对要求的对象、资源、应用等）权限声明者访问。为了保护系统的安全性，权限策略需要完整性和可靠性保护，防止他人通过修改权限策略而攻击系统。

2. PMI 技术的授权管理模式

授权服务体系主要是为网络空间提供用户操作授权的管理，即在虚拟网络空间中的用户

角色与最终应用系统中用户的操作权限之间建立一种映射关系。授权服务体系一般需要与信任服务体系协同工作，才能完成从特定用户的现实空间身份到特定应用系统中的具体操作权限之间的转换。目前建立授权服务体系的关键技术主要是授权管理基础设施技术。PMI 以资源管理为核心，对资源的访问控制权交由授权机构统一处理，即由资源的所有者来进行访问。

PMI 是一个由属性证书、属性权威、属性证书库等部件构成的综合系统，用来实现权限和证书的产生、管理、储存、分发和撤销等功能。PMI 使用属性证书表示和容纳权限信息，通过管理证书的生命周期实现对权限生命周期的管理。属性证书申请、签发、注销、验证的流程对应着权限申请、发放、撤销、使用和验证的过程，而且使用属性证书进行权限管理方式使得权限的管理不必依赖某个具体的应用，并有利于权限的安全分布式应用。

PMI 技术通过数字证书机制来管理用户的授权信息，并将授权管理功能从传统的应用系统中分离出来，以独立服务的方式面向应用系统提供授权管理服务。由于数字证书机制提供了授权信息的安全保护功能，因此作为用户授权信息存放载体的属性证书同样可以通过公开方式对外发布，由于属性证书并不提供用户身份的鉴别功能，因此属性证书中将不包含用户的公钥信息。

3. PMI 系统的架构

PMI 授权服务体系高度集中地管理用户和为用户授权，并且采用适当的用户身份信息来实现用户认证，主要是 PKI 体系下的数字证书，也包括动态口令或者指纹认证技术。安全平台将授权管理功能从应用系统中分离出来，以独立和几种服务的方式面向整个网络，统一为各应用系统提供授权管理服务。

授权管理基础设施 PMI 在体系结构上可以分为信任源点 SOA 中心、属性权威机构 AA 中心和 AA 代理点三级。在实际应用中，这种分级体系可以根据需要进行灵活配置，可以是三级、二级或一级，图 12-4 为权限管理基础设施的总体架构示意图。

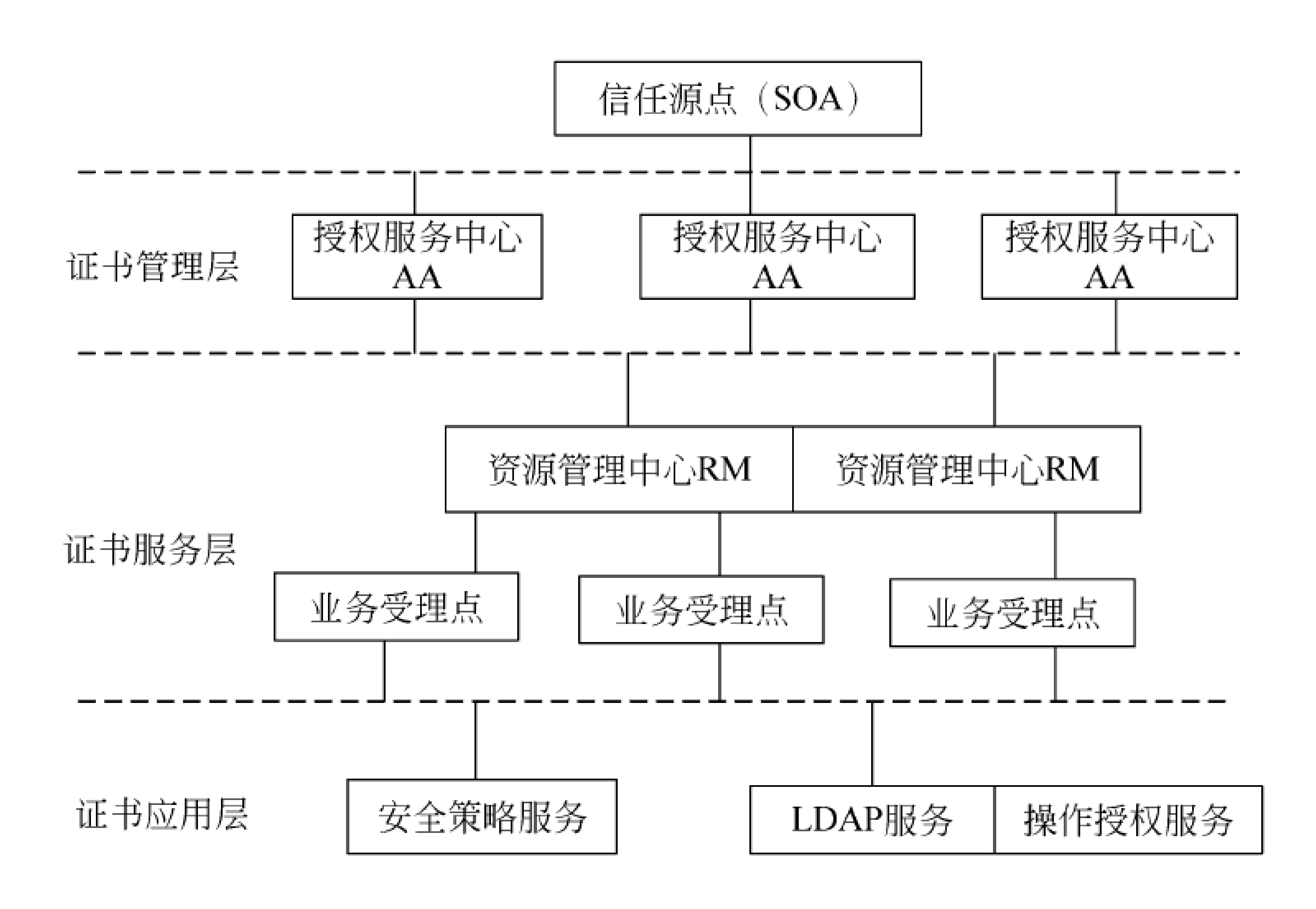


图 12-4　权限管理基础设施总体架构示意图

❑ **信任源点 SOA**

SOA 是整个授权管理体系的中心业务节点，也是整个授权管理基础设施的最终信任源和最高管理机构。

SOA 中心的职责主要包括授权管理策略的管理、应用授权受理、AA 中心的设立审核及管理和授权管理体系业务的规范化等。

❑ **属性权威机构 AA**

AA 是 PMI 的核心服务节点，对应于具体应用系统的授权管理分系统，由具有设立 AA 中心业务需求的各种应用单位负责建设，并与 SOA 中心通过业务协议达成相互信任的关系。

❑ **授权服务代理点**

授权服务代理点是 PMI 的用户代理节点，也称为资源管理中心，是与具体应用用户的接口，是对应 AA 中心的附属机构，接受 AA 中心的直接管理，由各 AA 中心负责建设，报经主管的 SOA 中心同意，并签发相应的证书。AA 代理点的设立和数目由各 AA 中心根据自身的业务发展需求而定。

❑ **访问控制执行者**

访问控制执行者是指用户应用系统中具体对授权验证服务的调用模块，因此实际上并不属于授权管理基础设施，但是却是授权管理体系的重要组成部分。

访问控制执行者的主要职责是：将最终用户针对特定的操作授权所提交的授权信息(属性证书)连同对应的身份验证信息（公钥证书）一起提交到授权服务代理点，并根据授权服务中心返回的授权结果，进行具体的应用授权处理。

4. PMI 系统的需求

在 PKI 的基础上，PMI 实际上提出了一个新的信息保护基础设施，能够与 PKI 和目录服务紧密地集成。PMI 作为一个基础设施能够系统地建立起对认可用户的授权。PMI 通过结合授权管理系统和身份认证系统补充了 PKI 的弱点，提供了将 PKI 集成到应用计算环境的模型。

一般来讲，PMI 权限管理和授权服务基础平台应该满足如下需求。

❑ 作为权限管理和授权服务的基础设施，可以为不同类型的应用提供授权管理和访问控制的平台支持。
❑ 平台策略的制定应该灵活，能够根据不同的情况制定出不同的策略。
❑ 平台管理功能的操作应该简单。
❑ 平台应该具有很好的扩展能力。
❑ 平台应该具有较好的效率，避免决策过程明显地影响访问速度。
❑ 平台应该独立于任何应用。

5. 授权管理基础设施 PMI 的应用

随着信息安全市场的成熟，对访问控制产品的兴趣和认识的日益增长，PMI 系统表现出了良好的应用前景。PMI 应用能够有效地增强系统的安全性，改变现有的多种权限管理模型带来的权限管理混乱状况，降低应用系统的开发成本，提高企业的效率。

❑ **在国家电子政务中应用**

国家信息安全基础设施（NISI）由公开密钥基础设施和授权管理基础设施组成。其中，公开密钥（简称“公钥”）基础设施构成所谓的 PKI 信息安全平台，提供智能化的信任服务；

而授权管理基础设施 PMI 构成所谓的授权管理平台，在 PKI 信息安全平台的基础上提供智能化的授权服务。

采用公钥密码体制构建公钥基础设施 PKI，是在大型开放的网络环境下解决信息安全问题的最可行、最有效的办法。公钥基础设施是国家信息安全建设中极其关键的基础性设施，它在底层网络基础设施的基础上构建了一个一致的信息安全服务层面，可以满足各种应用在安全方面的需求。

PMI 以一个身份鉴别体系（如 PKI 体系）为基础，向应用系统提供全面统一的授权管理和访问控制服务。授权管理基础设施 PMI 主要提供分布式计算环境中应用系统的访问控制功能，通过将访问控制机制从具体应用系统的开发和管理中分离出来，使访问控制机制与应用系统之间能灵活而方便地结合和使用。具有我国自主知识产权的授权管理基础设施现已研发成功。

可信时间戳服务系统是国家信息安全基础设施的另一重要组成部分，它将精确授时技术和公钥基础设施技术有机地结合起来，通过对证书或相关的数据加上时间标记，以此建立证据表明证书或数据的存在和有效性，从而为电子政务的各种应用提供可靠的时间戳服务。

授权管理基础设施 PKI 技术是一个新出现的领域，我国在这方面的研究比国外先进水平落后不多，由于电子政务应用自身的特点，PKI 技术将在整个电子政务系统中发挥重要作用。

❑ **基于 PKI/PMI 的 IP 宽带城域网安全应用**

采用 PKI/PMI 体系构建信任与授权服务支撑平台，为 IP 宽带城域网提供信任服务和授权服务。平台通过对实体的 PKC（包括用户个人信息，如序列号、IP 地址、MAC 地址等信息）和 AC（包括用户的属性信息，如角色、访问控制权限等）的认证、授权、管理来建立一个统一的智能化信任与授权基础环境，确立了“一实体一证、统一发证、分布式逐级管理”的 IP 宽带城域网运营管理模式。

其中，“一实体一证”是由 PKC 的唯一性，准确地标识用户身份；“统一发证”是指由第三方证书认证中心（CA）认证机构负责统一签发 IP 宽带城域网的用户、设备的 PKC，由信任与授权服务支撑平台提供 AC 的统一签发并实现证书的统一管理，保证网络信任域管理服务；“分布式逐级管理”是指按实际的责任和管理范围来划分网络信任域，每个城市或地区的 IP 宽带城域网系统也可以根据用户类型划分基本信任域（如可区别普通家庭用户、大客户等），每个基本信任域都由自己的管理系统负责本信任域的管理，网络信任域管理系统通过信任与授权服务支撑平台提供信任与授权服务的支持。以此模式构筑了一个责任明确、管理方便、覆盖全系统的网络信任域及管理体系。

例如，深圳电信采用了当今先进的网络产品和技术，充分开展各种先进的 IP 网络服务，代表了目前我国各大城市中最新的 IP 宽带城域网网络状况。该项目的关键技术是将我国具有自主知识产权的 PKI 和 PMI 等信息安全关键技术，应用到电信 IP 宽带网中来，构建了信息安全基础设施平台。其中采用数字证书方式实现电信宽带 IP 网络的用户认证和授权，从而实现 IP 宽带网的可控制、可管理、可经营。

12.5　属性权威和权限管理

权限管理基础设施 PMI 是一个由属性证书、属性权威、属性证书库等部件构成的综合系

统，用来实现属性证书的产生、管理、存储、分发和撤销等功能。

12.5.1　属性权威

属性权威（Attribute Authority，AA）是用来生成并签发属性证书（Attribute Certificate，AC）的机构。主要负责管理证书的整个生命周期。

AA 可划分为两种类型：一类相当于 SOA，可发布 AA 证书；一类则只发布属性证书，不能发布 AA 证书。

AA 负责对最终实体或者其他属性管理机构进行授权。在授予一种特权之前，该 AA 必须已经拥有该特权。也就是说该 AA 必须已经被授予是这项权力或者这项特权的源头。

另外，AA 也可能需要为其发布的证书签发撤销通知。但对于短生命周期的证书来讲，撤销通知是不必要的，因此通常并不要求发布撤销通知。然而，AA 需要标识其签发的证书是否补充撤销信息，如果是，那么还应该包含其存放位置。

AA 和 CA 在逻辑上完全独立。身份的创建和维护应该与 PMI 分离开来，因此一个完整的 PKI 包括 CA，可能在 PMI 建立之前已经存在并且可用。尽管 CA 是域身份权威的源，但它不是自动权限的权威源，因此，CA 本身不必是 AA。

在实际应用 PMI 系统构建安全应用时，属性权威 AA 的能力和应用方式可以根据具体的建设要求和成本来灵活确定。例如，在一个较小的网络应用中，系统的使用人员和资源较少，可以采用嵌入式的属性权威 AA 签发和管理属性证书，从而减少建设成本和管理开销。而在一个由多个应用组成的较大系统中，则存在着大量的用户和资源，并对系统的整体安全性有很高的要求，此时可以考虑建立属性权威中心将所有的应用划分到同一个安全域中，由 PMI 的整体安全策略和授权策略来实现整个系统范围内的所有应用的整体安全访问。这样，不仅可以减少属性权威 AA 的重复性投资，而且可以通过较为集中的管理模式减少管理的复杂性和开销，并带来更好的全局安全性。

一般来讲，一个属性权威 AA 主要由 AC 签发、受理和管理、数据库服务器、目录服务器几部分组成，其中数据库服务器不是必需的，图 12-5 为 AA 结构示意图。其中，各组成部分有以下说明。

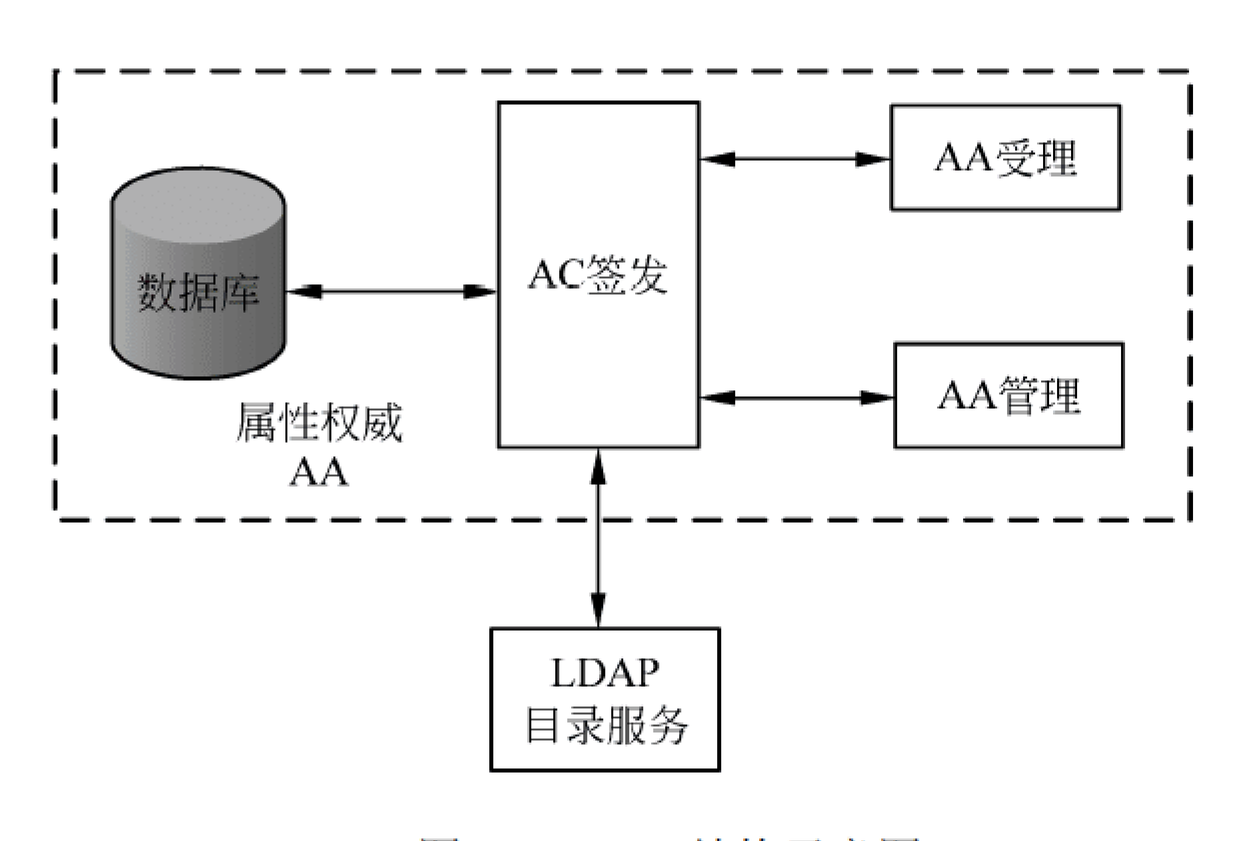
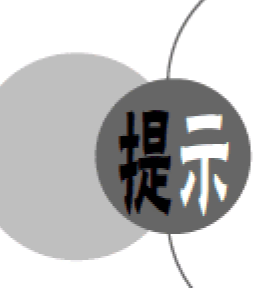


图 12-5　AA 结构示意图

- ❑ **AC 签发** 该服务是属性权威 AA 的主体，是以 PKI 技术为基础，以授权服务为主要任务的服务模块，用于签发属性证书，该服务可以由一台独立的服务器提供，也可以由证书签发模块提供。
- ❑ **AA 受理** 主要用于接受并验证对属性证书的请求，以及处理该请求，提供基于属性证书的授权服务、基于属性证书的委托服务等。
- ❑ **AA 管理** 用于管理属性权威 AA。
- ❑ **数据库** 主要是用于存储用户和资源的基本信息，也可以将这些信息直接放入 LDAP 目录服务器中。
- ❑ **LDAP 目录服务器** 主要用于发布 PMI 用户的属性证书以及属性证书的撤销列表（Attribute Certificate Revocation List，ACRL），以供查询使用。该服务器可以直接存放用户和资源信息，这样可以不使用数据库存放这些信息。



在企业或公司网络中，各业务应用系统在创建属性权威 AA 时，应该根据系统内用户的数量及管理模式来确定 AA 属性权威、LDAP 服务器的服务能力，并相应地确定与当前系统相适应的服务能力冗余备份和性能扩展方案，以确保整个 PMI 服务能力具有延续性和良好的业务量适应能力。

12.5.2 权限管理

权限管理和访问控制是信息安全保障机制的核心内容，它是实现数据保密性和完整性的主要手段，限制访问主体（如用户、进程、服务等）对访问客体（需要保护的资源）的访问权限，从而使计算机系统在合法范围内使用。

1. 为什么要进行权限管理

传统的应用系统通常是通过使用“用户名＋口令”的方式来控制用户对应用系统的访问权限。系统通过验证用户在登录系统时输入的用户名和口令来确定用户的身份，同时，通过维护一张访问控制列表 ACL 确定每个用户对特定系统对象的操作权限。这种方法因为简便易行而得到了普遍的应用。但是，对于一些大型的企业或公司来说，其网络结构比较复杂，应用系统较多，用户数量巨大，采用这种方式需要不同的应用系统分别针对其保护的资源进行权限的管理和控制，会产生以下几个问题。

❑ **权限管理混乱**

对一个组织机构而言，数据和人力资源是统一的。但是由于系统设计的原因，可能同时对相同的人员采用不同的管理方式，对机构内的共享数据采用不同的权限分配策略，这显然不合理，也不利于对机构资源的管理。

❑ **系统安全性较低**

不同的权限管理策略产生的安全强度不同，这就可能造成机构信息安全管理的漏洞，入侵者就有可能针对那些权限管理相对不安全的系统进行集中攻击，给资源的安全性带来极大的危害。

- **权限管理依赖于访问控制应用**

权限的赋予和撤销都是在访问控制应用中产生的，不同的访问控制应用之间尽管有相同的用户和授权策略却不能互相使用对方产生的权限。每个应用都要维护自己的用户信息和授权方法，权限无法在分布的应用中和远程应用中使用。

- **资源所有者没有权限**

应用系统负责权限的发放和使用，造成权限真正的拥有者不能及时有效地更改和发布实时的权限信息。比如，机构内一个人职务或业务的变化必须通知相关的不同应用分别进行更新。从本质上讲，权限的发放和权限的鉴别使用是完全不同的两个过程，完全可以分开，权限的拥有者发放权限，而由资源的保护者验证权限。

- **增加了系统管理员的负担**

由于不同的系统采用的是不同的权限管理策略，系统管理员不得不熟悉和操作不同的权限管理模式，这无疑增加了系统管理员的负担。另外，对于大型复杂的应用系统采用权限访问控制列表的方式来分配权限，也给系统管理员带来巨大负担且容易出错。

- **开发复杂且费用高**

设计一个新的安全应用系统时，权限管理是一个极其重要的部分。在缺乏统一的权限管理模型的情况下，设计人员要考虑选择何种权限管理模型和访问控制授权方案，而且开发人员也要根据不同的应用花费较大的代价来实现权限管理功能。

2. PMI 权限管理

在权限管理系统中也存在安全策略管理的问题，同一权限管理系统将遵循相同的安全策略提供权限管理服务，不同的权限管理系统之间的互通必须以策略的一致为前提。

在 PMI 中采用基于角色的权限管理（Role Based Access Control，RBAC）技术，它的特点是通过将一组权限赋予角色，将角色赋予使用者的二级映射模式，使角色成为权限与使用者之间多对多映射的纽带。基于角色的权限管理防止了用户和权限直接相关联，使授权过程与具体的应用相分离，是目前公认的解决大型组织的统一资源权限管理的有效方法。

基于角色的权限管理定义了以下 5 个基本要素。

- 访问对象（Objects）指包含或接收信息的对象，是权限管理系统保护的资源。
- 操作（Operations）指对一个或多个访问对象执行的指令，操作的类型与访问的对象有关。
- 使用者（Users）指使用访问控制系统试图操作访问对象的人。
- 权限（Permissions）指对一个或多个访问对象的操作的许可。
- 角色（Roles）指一个组织或任务中的工作或位置，它代表了一种资格、权利和责任。

另外，基于角色的权限管理的实行包括如下 3 个阶段。

- **权限定义**　资源的拥有者为每个访问对象设置可执行的操作，形成权限。
- **角色定义**　定义组织中的各个角色名称，并将角色与确定权限绑定在一起。一个角色可以拥有多个权限，一个权限可以赋予多个角色。
- **角色分配**　将使用者与角色绑定在一起，则该使用者拥有该角色所对应的权限，可以对访问对象进行权限中允许的操作。一个使用者可以赋予多个角色，一个角色可以被赋予多个权限。

与传统的权限管理模式相比，基于 PMI 技术的权限管理模式主要存在以下 3 个方面的

优势。

❑ 权限管理的灵活性

基于 PMI 技术的权限管理模式可以通过属性证书的有效期以及委托授权机制来灵活地进行权限管理，实现了强制访问控制模式与自主访问控制模式的有机结合。采用属性证书机制的权限管理技术对授权管理信息提供了更多的保护功能。

❑ 权限操作与业务操作相分离

基于 PMI 技术的权限管理模式将业务管理工作与权限管理工作完全分离，更加明确业务管理员和安全管理员之间的职责分工，可以有效地避免由于业务管理人员参与到权限管理活动中而带来的一些问题。

❑ 多权限模型的灵活支持

基于 PMI 技术的权限管理模式将整个权限管理体系从应用系统中分离出来，权限管理模块自身的维护和更新操作将与具体的应用系统无关，可以在不影响原有应用系统正常运行的前提下，实现对多权限模型的支持。

12.6　基于 PMI 建立安全应用

在过去的几年里，PKI 已经成为电子商务、企业办公等网络应用中不可或缺的安全支撑系统。它通过方便灵活的密钥和证书管理方式，提供了在线身份认证的有效手段，为访问控制系统、抗抵赖、保密性等安全机制在系统中的实施奠定了基础。

随着网络应用的深入和发展，仅仅能够确定“他是谁”已经不能够满足当今的需要，安全系统要求能够提供一种手段进一步确定“他能做什么”，因此，基于 PMI 建立安全应用变得尤为重要。

12.6.1　PMI 应用结构

PMI 作为一个基础设施能够系统地建立起对认可用户的授权。通过结合授权管理系统和身份认证系统补充了 PKI 的弱点。PMI 作为权限管理和授权服务的基础设施，可以为不同类型的应用提供授权管理和访问控制的平台支持。

PMI 建立在 PKI 提供的可信身份认证服务的基础上，以属性证书的形式实现授权的管理，PMI 体系和模型的核心内容是实现属性证书的有效管理，包括属性证书的产生、使用、吊销、失效等。

一般来讲，与 PKI 相同，PMI 同样由多个部分组成，并由这些部分构成了自身的应用结构，图 12-6 为 PMI 应用结构示意图。

在 PMI 应用结构中，有关各部分的说明如下。

❑ 访问者、目标

访问者是一个实体（该实体可能是人，也可能是其他计算机实体），它试图访问系统内的其他实体（目标）。

PKI
为用户签发身份证书
为AA签发身份证书
访问者
策略实施
目标
策略决策 PDP
策略
注册申请 ARA
属性权威AA
LDAP
应用系统
应用策略支撑框架
属性证书签发系统

图 12-6 PMI 应用结构示意图

❑ **策略**

授权策略展示了一个机构在信息安全和授权方面的顶层控制以及授权遵循的原则和具体的授权信息。在一个机构的 PMI 应用中，策略应当包括一个机构如何将它的人员和数据进行分类组织，这种组织方式应该考虑到具体应用的实际运行环境，如数据的敏感性、人员权限的明确划分以及必须和相应人员层次相匹配的管理层次等因素。所以策略的制定需要根据具体的应用量身定做。

具体地说，策略包含着应用系统中的所有用户和资源信息以及用户和信息的组织管理方式；用户和资源之间的权限关系；保证安全的管理授权约束；保证系统安全的其他约束。在 PMI 中主要使用基于角色的访问控制（RBAC，Role-Based Access Control）。

❑ **属性证书（AC）**

AC 是 PMI 的基础概念，它是权威签名的数据结构，将权限和实体信息绑定在一起。属性证书中包含了用户在某个具体的应用系统中的角色信息，而该角色具有什么样的权限是在策略中制定的。

❑ **AA**

属性证书的签发者称为属性权威（AA），属性权威 AA 的根称为信任源点 SOA。

❑ **ARA**

属性证书的注册申请机构称为属性注册权威 ARA。

❑ **LDAP**

用来存储签发的属性证书和属性证书撤销列表。

❑ **策略实施**

策略实施点（Policy Enforcement Points，PEPs）也称为 PMI 激活的应用，对每一个具体的应用可能是不同的，是指已经通过接口插件或者代理所修改过的应用或者服务。这种应用或服务被用来实施一个应用内部的策略决策，介于访问者和目标之间，当访问者申请访问时，策略实施点向授权策略服务器申请授权，并根据授权决策的结果实施决策，即对目标执行访问或者拒绝访问。在具体的应用中，策略实施点可能是应用程序内部中进行访问控制的一段

代码，也可能是安全的应用服务器（如在 Web 服务器上增加一个访问控制插件），或者是进行访问控制的安全应用网关。

❑ **策略决策**

策略决策点（Policy Decision Point，PDP）也叫授权策略服务器，它接收和评价授权请求，根据具体策略做出不同的决策。它一般不随具体的应用而发生变化，是一个通用的处理判断逻辑。当接收到一个授权请求时，根据授权的策略、访问者的安全属性以及当前条件进行决策，并将决策结果返回给应用。对于不同应用的支持是通过解析不同的定制策略来完成的。

12.6.2　访问控制模型

访问控制是网络安全防范和保护的核心策略，它的主要任务是保证网络资源不被非法使用和访问。访问控制规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以控制。它是对信息系统资源进行保护的重要措施，也是计算机系统最重要和最基础的安全机制。

1. 自主访问控制模型

自主访问控制模型（Discretionary Access Control Model，DAC Model）是根据自主访问控制策略建立的一种模型，允许合法用户以用户或用户组的身份访问策略规定的客体，同时阻止非授权用户访问客体，某些用户还可以自主地把自己所拥有的客体的访问权限授予其他用户。

自主访问控制又称为任意访问控制。在 Linux，UNIX、Windows NT 或是 Server 版本的操作系统中都有自主访问控制的功能。在实现上，首先要对用户的身份进行鉴别，然后就可以按照访问控制列表所赋予用户的权限允许和限制用户使用客体的资源。主体控制权限的修改通常由特权用户或是特权用户（管理员）组实现。

任意访问控制对用户提供的这种灵活的数据访问方式，使得 DAC 广泛应用在商业和工业环境中。例如，由于用户可以任意传递权限，那么，没有访问文件 File1 权限的用户就能够从有访问权限的用户那里得到访问权限或是直接获得文件 File1。因此，DAC 模型提供的安全防护还是相对比较低的，不能给系统提供充分的数据保护。

自主访问控制模型的特点是授权的实施主体（可以授权的主体、管理授权的客体和授权组）自主负责赋予和回收其他主体对客体资源的访问权限。DAC 模型一般采用访问控制矩阵和访问控制列表来存放不同主体的访问控制信息，从而达到对主体访问权限的限制目的。

2. 强制访问控制模型

强制访问控制模型（Mandatory Access Control Model，MAC Model）最初是为了实现比 DAC 更为严格的访问控制策略，美国政府和军方开发了各种各样的控制模型，这些方案或模型都有比较完善和详尽的定义。随后，逐渐形成强制访问控制模型，并得到广泛的商业关注和应用。

在 DAC 访问控制中，用户和客体资源都被赋予一定的安全级别，用户不能改变自身和客体的安全级别，只有管理员才能确定用户和组的访问权限。和 DAC 模型不同的是，MAC 是

一种多级访问控制策略，其主要特点是系统对访问主体和受控对象实行强制访问控制，系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。

MAC 对访问主体和受控对象标识了具有偏序关系的安全等级标记和非等级分类标记两个安全标记。主体和客体在分属不同的安全类别时，都属于一个固定的安全类别 SC，SC 就构成一个偏序关系（比如 TS 表示绝密级，就比密级 S 要高）。当主体的安全类别为 TS，而客体的安全类别为 S 时，用偏序关系可以表述为 SC（s）≥SC（o）。考虑到偏序关系，主体对客体的访问主要有 4 种方式。

- **向下读（read down，rd）** 主体安全级别高于客体信息资源的安全级别时允许查阅的读操作。
- **向上读（read up，ru）** 主体安全级别低于客体信息资源的安全级别时允许的读操作。
- **向下写（write down，wd）** 主体安全级别高于客体信息资源的安全级别时允许执行的动作或是写操作。
- **向上写（write up，wu）** 主体安全级别低于客体信息资源的安全级别时允许执行的动作或是写操作。

由于 MAC 通过分级的安全标签实现了信息的单向流通，因此它一直被军方采用，其中最著名的是 Bell-LaPadula 模型和 Biba 模型。Bell-LaPadula 模型具有只允许向下读、向上写的特点，可以有效地防止机密信息向下级泄露；Biba 模型则具有不允许向下读、向上写的特点，可以有效地保护数据的完整性。

3．基于角色的访问控制模型

基于角色的访问控制模型（Role-based Access Model，RBAC Model）将访问许可权分配给一定的角色，用户通过扮演不同的角色获得角色所拥有的访问许可权。这是因为在很多实际应用中，用户并不是可以访问的客体信息资源的所有者（这些信息属于企业或公司），这样的话，访问控制应该基于员工的职务而不是基于员工在哪个组，即访问控制是由各个用户在部门中所担任的角色来确定的，例如，一个学校可以有教工、老师、学生和其他管理人员等角色。

RBAC 从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色相联系，这点与传统的 MAC 和 DAC 将权限直接授予用户的方式不同；通过给用户分配合适的角色，让用户与访问权限相联系。角色成为访问控制中访问主体和受控对象之间的一座桥梁。

角色可以看作是一组操作的集合，不同的角色具有不同的操作集，这些操作集由系统管理员分配给角色。例如，Tch1，Tch2，Tch3，…，Tchi 对应不同的教师；Stud1，Stud 2，Stud3，…，Studj 对应不同的学生；Mng1，Mng 2，Mng 3，…，Mngk 对应不同的教务处管理人员；教师的权限为 TchMN={查询成绩、上传所教课程的成绩}；学生的权限为 Stud MN={查询成绩、反映意见}；教务管理人员的权限为 MngMN={查询、修改成绩、打印成绩清单}。那么根据角色的不同，每个主体只能执行自己所制定的访问功能。用户在一定的部门中具有一定的角色，其所执行的操作与其所扮演的角色的职能相匹配，这正是基于角色的访问控制的根本特征。也就是说根据 RBAC 策略，系统定义了各种角色，每种角色可以完成一定的职能，不同的用

户根据其职能和责任被赋予相应的角色，一旦某个用户成为某角色的成员，则此用户可以完成该角色所具有的职能。

系统管理员负责授予用户各种角色的成员资格或撤销某用户具有的某个角色。例如，学校新进一名教师 Tchx，那么系统管理员只需将 Tchx 添加到教师这一角色的成员中即可，而无需对访问控制列表做改动。同一个用户可以是多个角色的成员，即同一个用户可以扮演多种角色，比如，一个用户可以是老师，同时也可以作为进修的学生。同样，一个角色可以拥有多个用户成员（这与现实是一致的）。一个人可以在同一部门中担任多种职务，而且担任相同职务的可能不止一人。因此 RBAC 提供了一种描述用户和权限之间的多对多关系，角色可以划分成不同的等级，通过角色等级关系来反映一个组织的职权和责任关系，这种关系具有反身性、传递性和非对称性等特点，通过继承行为形成一个偏序关系，比如 MngMN>TchMN>Stud MN。

RBAC 中通常定义不同的约束规则来对模型中的各种关系进行限制，最基本的约束是“相互排斥”约束和“基本限制”约束，它们分别规定了模型中的互斥角色和一个角色可被分配的最大用户数。RBAC 中引进了角色的概念，用角色表示访问主体具有的职权和责任，灵活地表达和实现企业的安全策略，使系统权限管理在企业的组织视图这个较高的抽象集上进行，从而简化权限设置的管理，从这个角度看，RBAC 很好地解决了企业管理信息系统中用户数量多、变动频繁的问题。

相比较而言，RBAC 是实施面向企业的安全策略的一种有效的访问控制方式，其具有灵活性、方便性和安全性的特点，目前在大型数据库系统的权限管理中得到普遍应用。角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。用户与客体无直接联系，他只有通过角色才享有该角色所对应的权限，从而访问相应的客体。因此用户不能自主地将访问权限授予其他用户，这是 RBAC 与 DAC 的根本区别。另外，RBAC 与 MAC 的区别还在于 MAC 是基于多级安全需求的，而 RBAC 则不是。

12.6.3　访问控制实现

访问控制是网络安全防范和保护的重要手段，它的主要任务是维护网络系统安全、保证网络资源不被非法使用和非正常访问。通常在技术实现上，包括以下几个部分。

1．接入访问控制

接入访问控制为网络访问提供了第一层访问控制，是网络访问的最先屏障，它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。例如，ISP 服务商实现的就是接入服务。用户的接入访问控制是对合法用户的验证，通常使用用户名和口令的认证方式。一般可分为用户名的识别与验证、用户口令的识别与验证和用户账号的默认限制检查这 3 个步骤。

2．资源访问控制

资源访问控制是对客体整体资源信息的访问控制管理。其中包括文件系统的访问控制（文

件目录访问控制和系统访问控制)、文件属性访问控制、信息内容访问控制。其中，文件目录访问控制是指用户和用户组被赋予一定的权限，在权限的规则控制许可下，哪些用户和用户组可以访问哪些目录、子目录、文件和其他资源，哪些用户可以对其中的哪些文件、目录、子目录、设备等执行何种操作。

系统访问控制是指一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问；应设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；应设定服务器登录时间限制、非法访问者检测和关闭的时间间隔；应对网络实施监控，记录用户对网络资源的访问，对非法的网络访问，能够用图形或文字或声音等形式报警等。

文件属性访问控制是指当用文件、目录和网络设备时，应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与要访问的文件、目录和网络设备联系起来。

3. 网络端口和节点的访问控制

网络中的节点和端口往往加密传输数据，这些重要位置的管理必须防止黑客发动的攻击。对于管理和修改数据，应该要求访问者提供足以证明身份的验证器（如智能卡）。

12.7 操作实例——使用 SSL 搭建安全的 Web 站点

网站安装证书并启用 SSL 功能，建立安全的访问连接，能够确保用户信息的正确性，将用户与网站之间的信息加密，防止重要信息外泄，同时可防止数据在传递过程中，被拦截或篡改，保证信息完整性。

1. 实例目的

- 从 CA 服务器申请证书。
- 下载证书。
- Web 与证书绑定。

2. 实例步骤

（1）在桌面上，执行【开始】|【运行】命令，在【打开】文本框中，输入 http://127.0.0.1/certsrv/default.asp 命令，并单击【确定】按钮，如图 12-7 所示。

（2）在【欢迎使用】窗口中，选择【申请证书】选项，如图 12-8 所示。

（3）在【申请一个证书】窗口中，选择【Web 浏览器证书】选项，如图 12-9 所示。

（4）在【Web 浏览器证书-识别信息】窗口的文本框中，依次输入相应信息，并单击【提交】按钮，如图 12-10 所示。

（5）在 CA 服务器桌面上，执行【开始】|【程序】|【管理工具】|Certification Authority 命令，并在 certsrv-【证书颁发机构（本地）\My CA\挂起的申请】窗口主界面中，展开 My CA 节点，如图 12-11 所示。

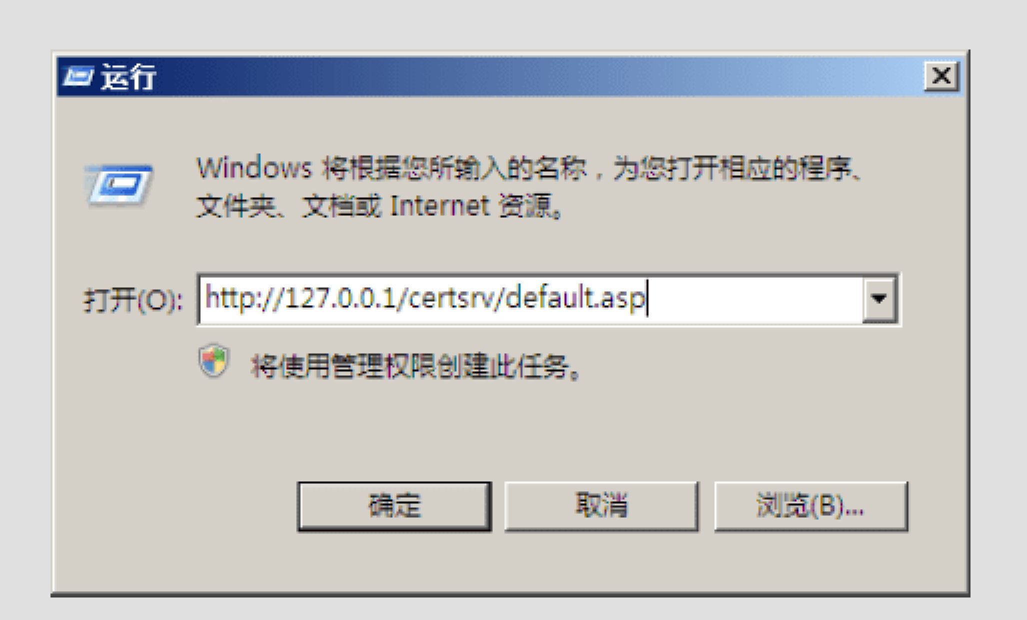


图 12-7 【运行】对话框

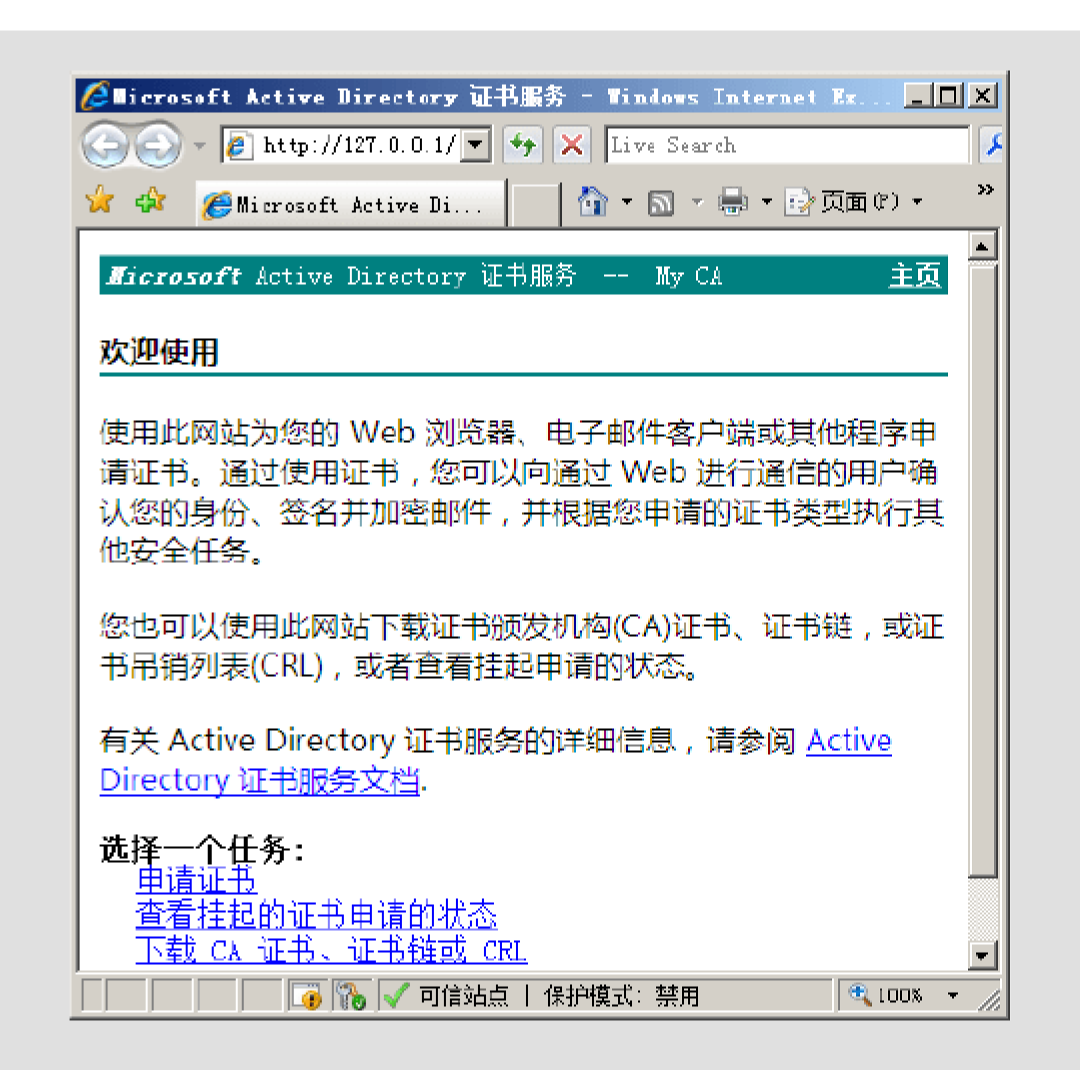


图 12-8　申请证书窗口

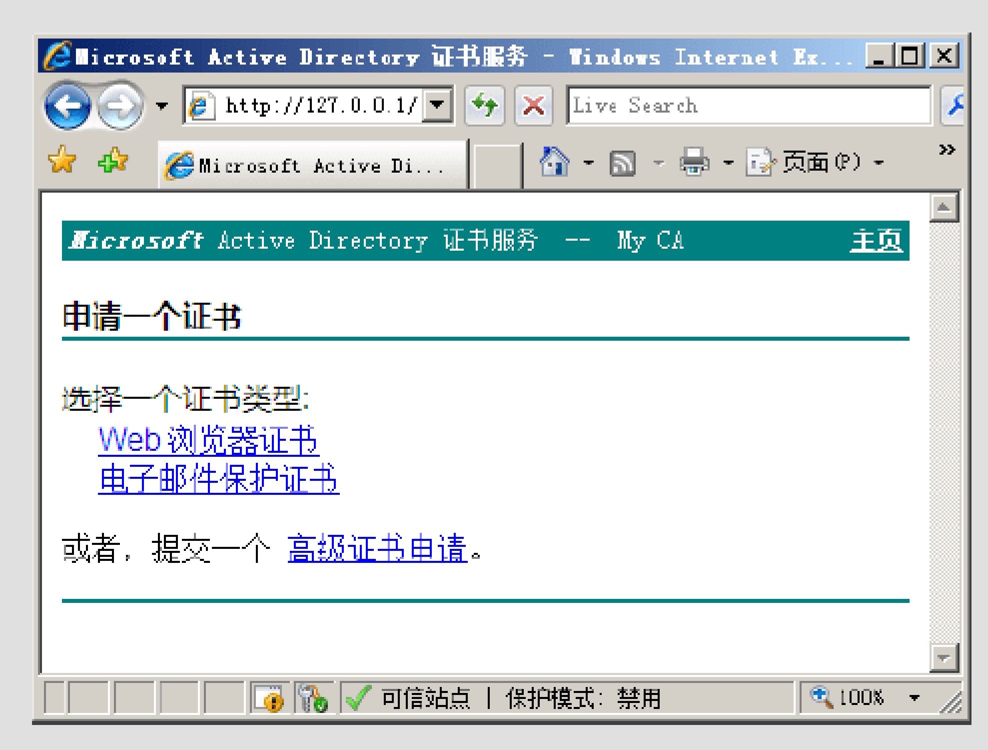


图 12-9　【申请一个证书】窗口

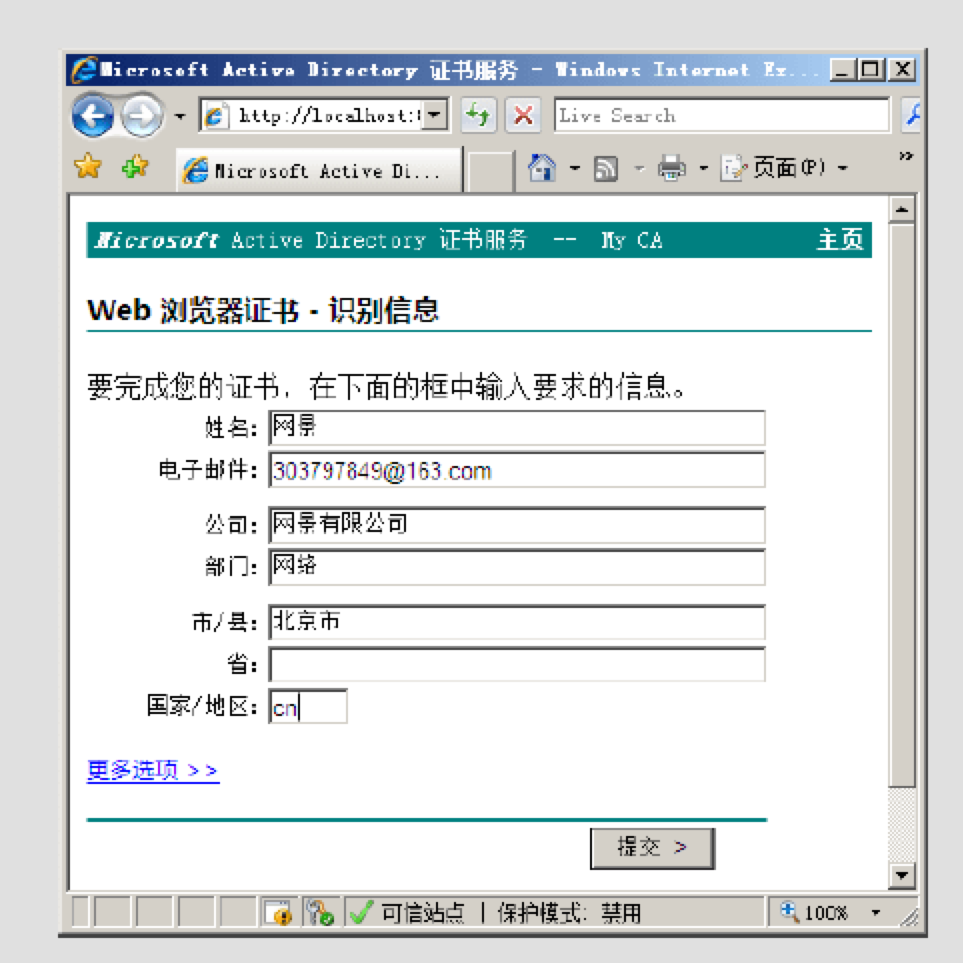


图 12-10 【Web 浏览器证书-识别信息】窗口

（6）选择【挂起的申请】选项，并在右侧窗格内右击申请 ID 为 3 的证书，执行【所有任务】|【颁发】命令，如图 12-12 所示。

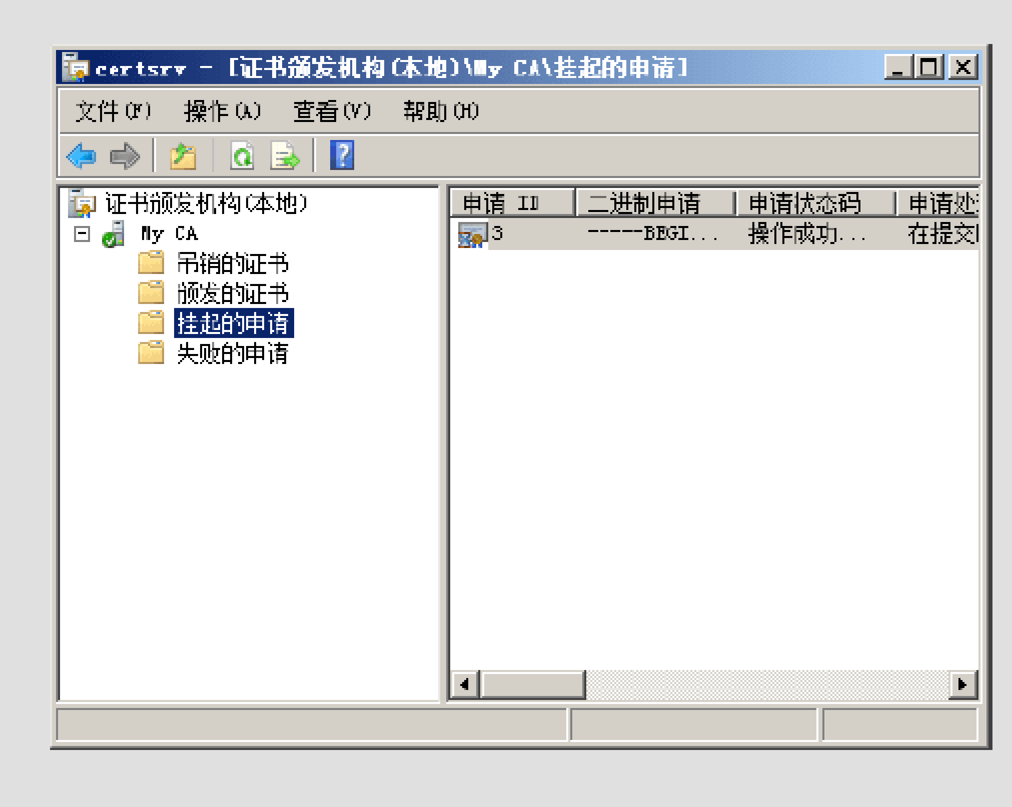


图 12-11　证书颁发机构窗口

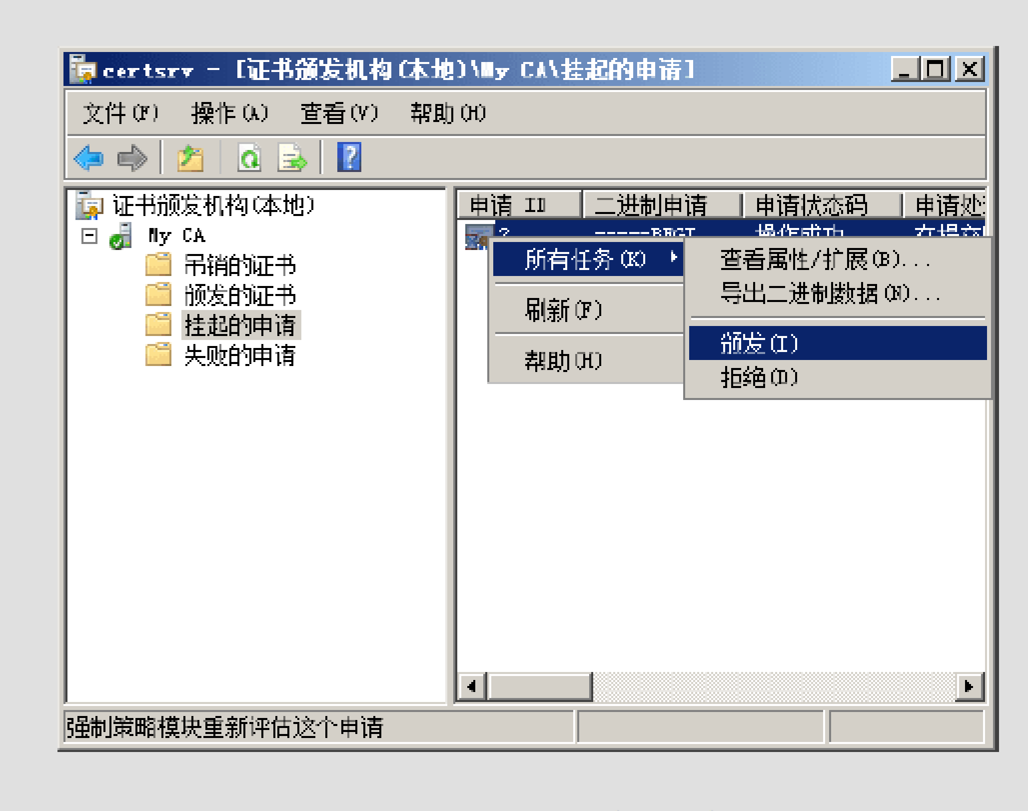


图 12-12　颁发证书

（7）在桌面上，执行【开始】|【运行】命令，在【打开】文本框中，输入 http://127.0.0.1/certsrv/default.asp命令并单击【确定】按钮，如图 12-13 所示。

（8）在【欢迎使用】窗口中，选择【下载 CA 证书、证书链或 CRL】选项，如图 12-14 所示。

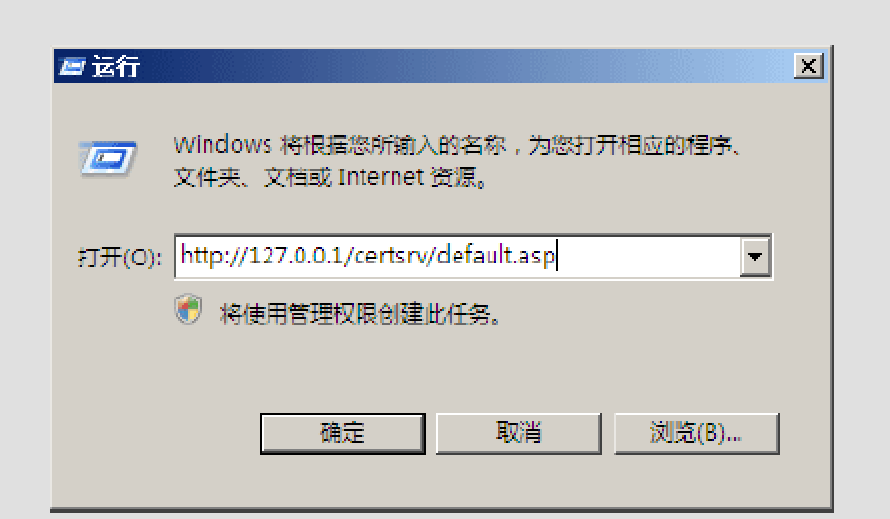


图 12-13 【运行】对话框

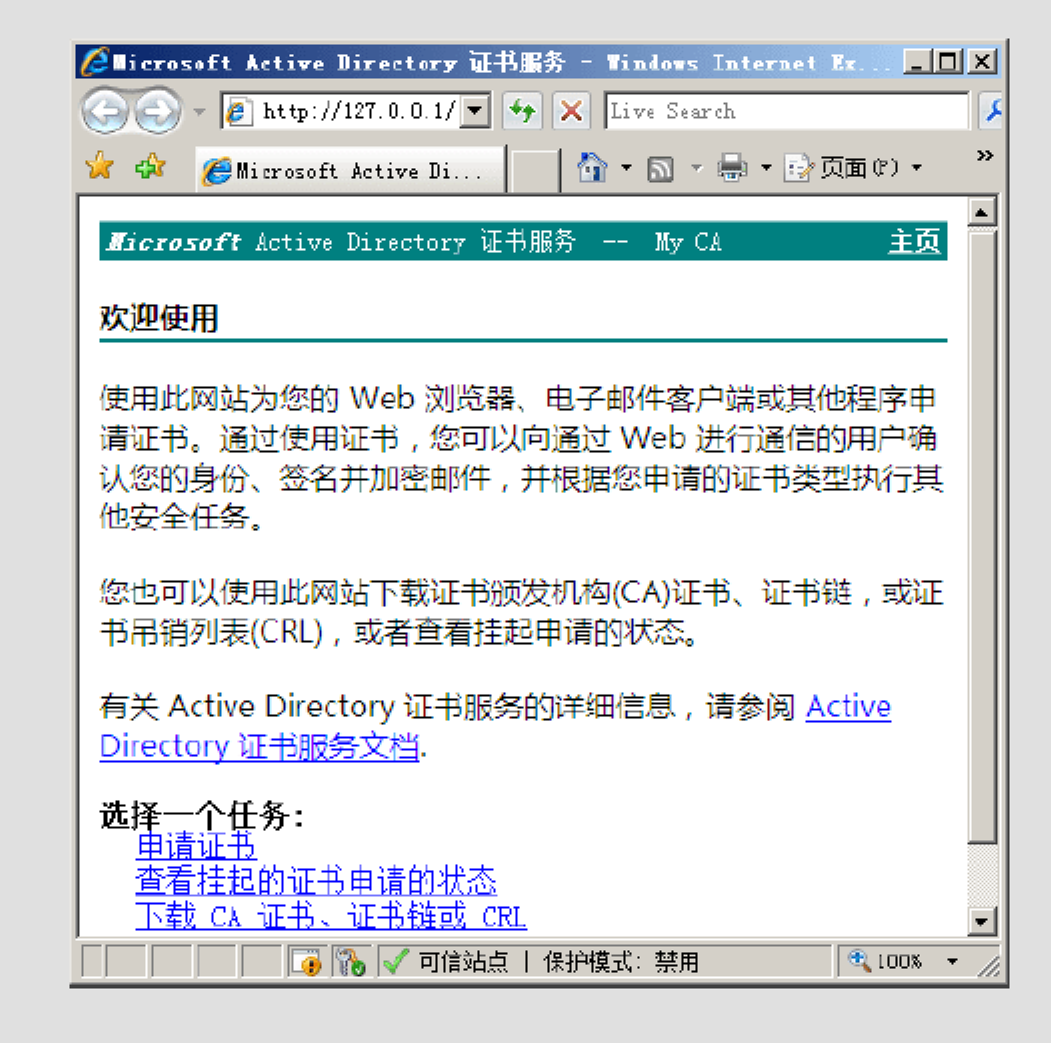


图 12-14 下载证书

（9）在【下载 CA 证书、证书链或 CRL】窗口中，选择【下载 CA 证书】选项，如图 12-15 所示。

（10）在弹出的【文件下载-安全警告】对话框中，单击【保存】按钮，如图 12-16 所示。

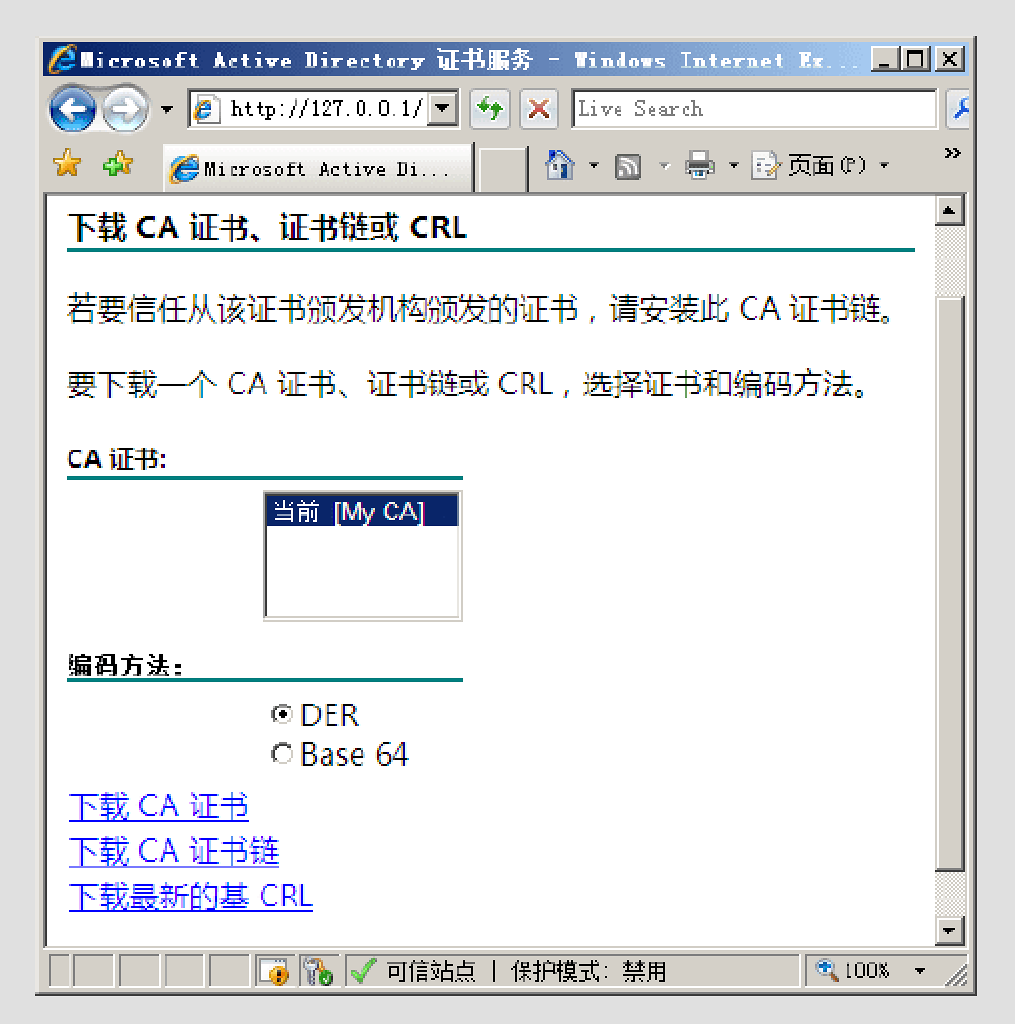


图 12-15 下载 CA 证书窗口

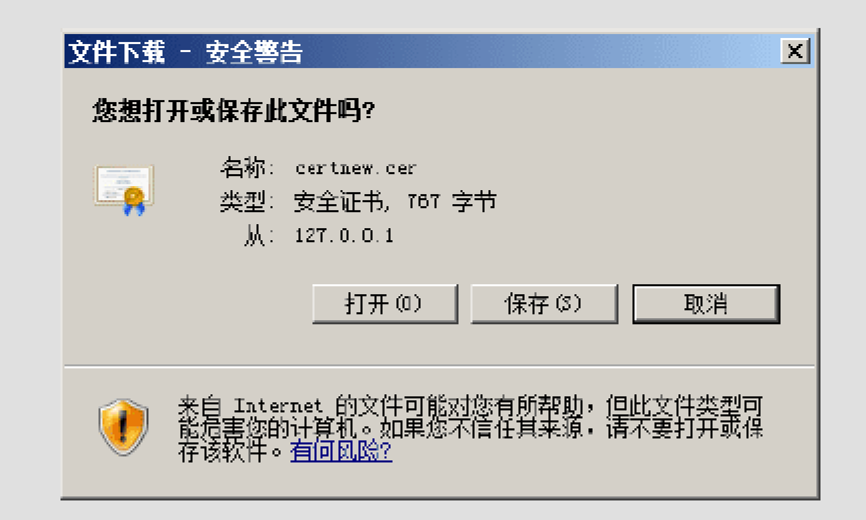


图 12-16 保存证书

（11）在弹出的【另存为】对话框中，单击【保存】按钮，如图 12-17 所示。

（12）在【下载完毕】窗口中，单击【关闭】按钮，如图 12-18 所示。

（13）在桌面上，执行【开始】|【运行】命令，在【打开】文本框中，输入 inetmgr 命令，并单击【确定】按钮，如图 12-19 所示。

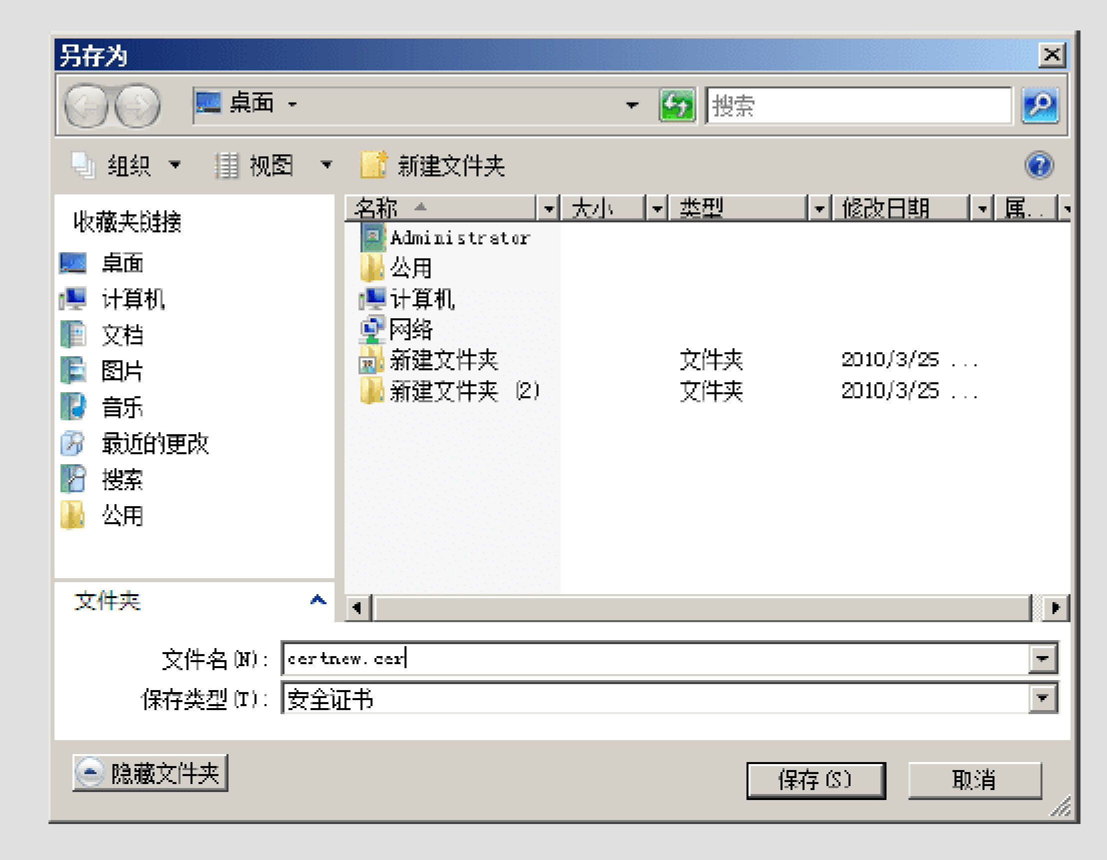



图 12-17　【另存为】对话框

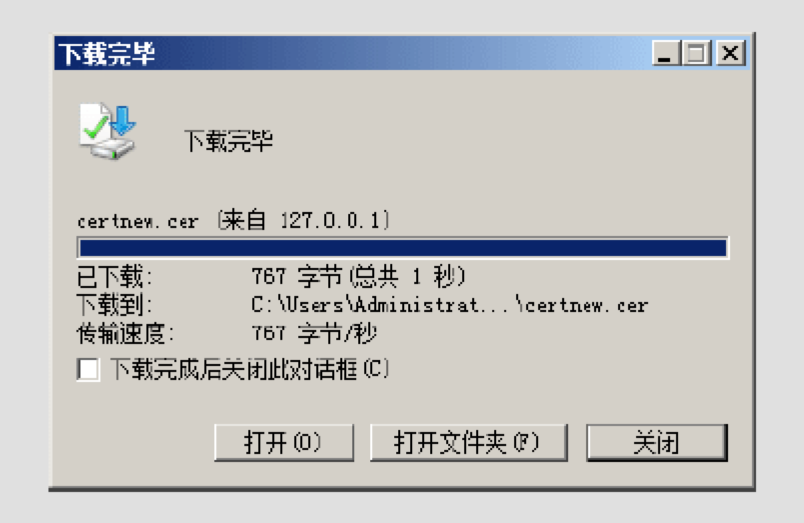
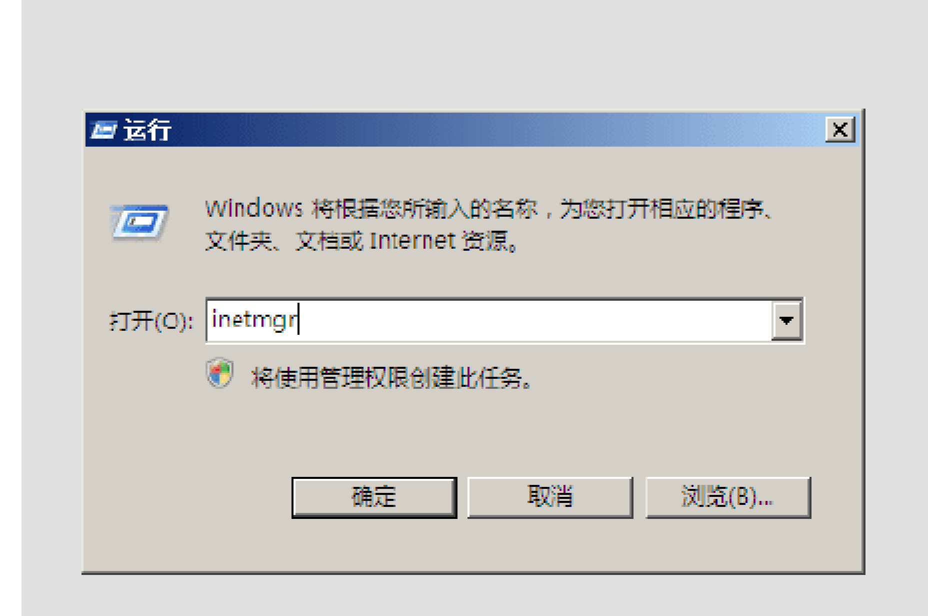


图 12-18　【下载完毕】窗口

（14）在【Internet 信息服务（IIS）管理器】窗口中，依次展开 WIN-TW2PIHFW477(WIN)|【网站】节点，并右击 mytext 选项，执行【编辑绑定】命令，如图 12-20 所示。



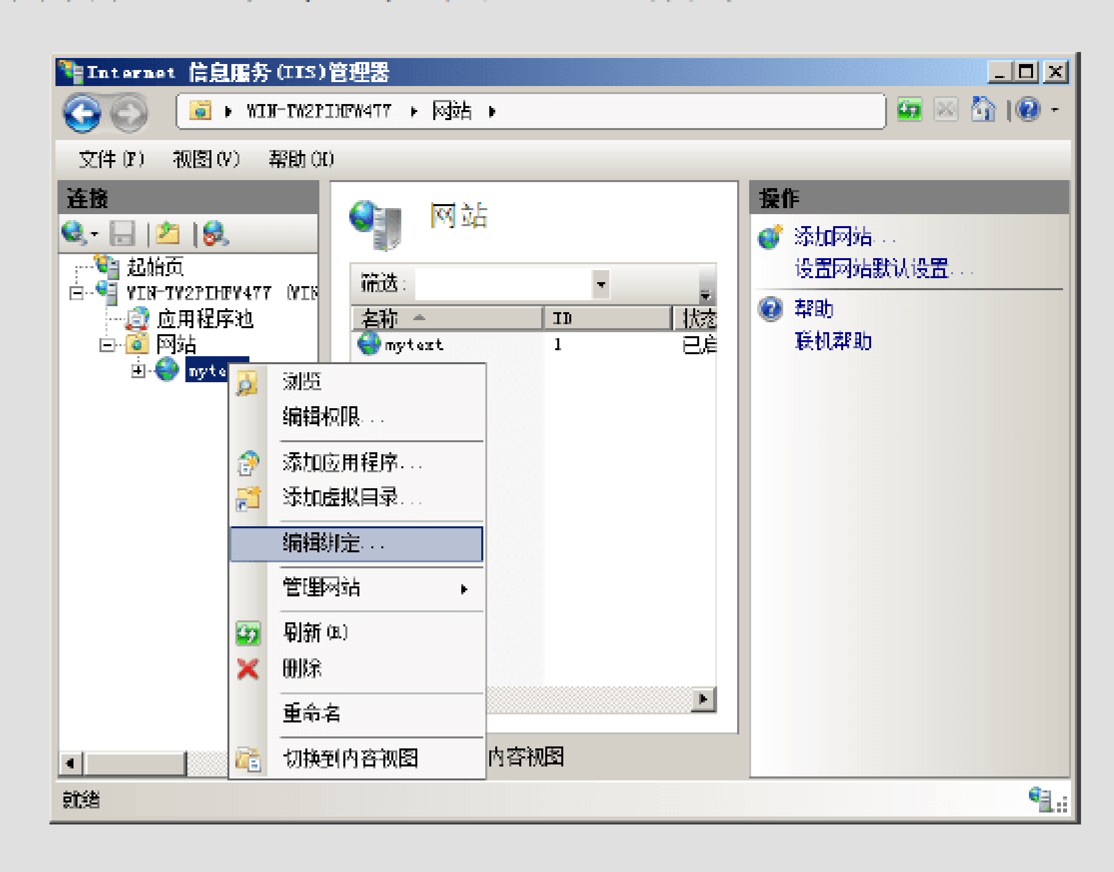
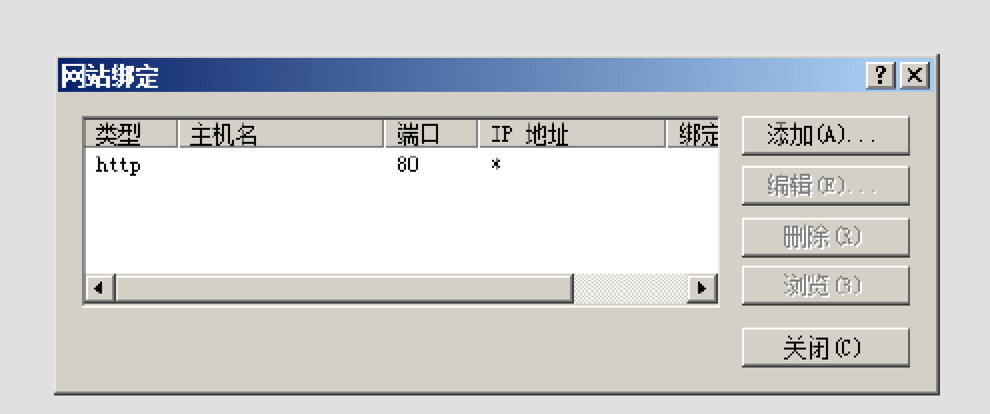


图 12-19　【运行】对话框

图 12-20　【Internet 信息服务（IIS）管理器】窗口

（15）在【网站绑定】对话框中，单击【添加】按钮，如图 12-21 所示。

（16）在弹出的【添加网站绑定】对话框中，单击【类型】下拉按钮，选择 https 选项，并单击【SSL 证书】下拉按钮，选择 My CA 选项，然后单击【确定】按钮，如图 12-22 所示。



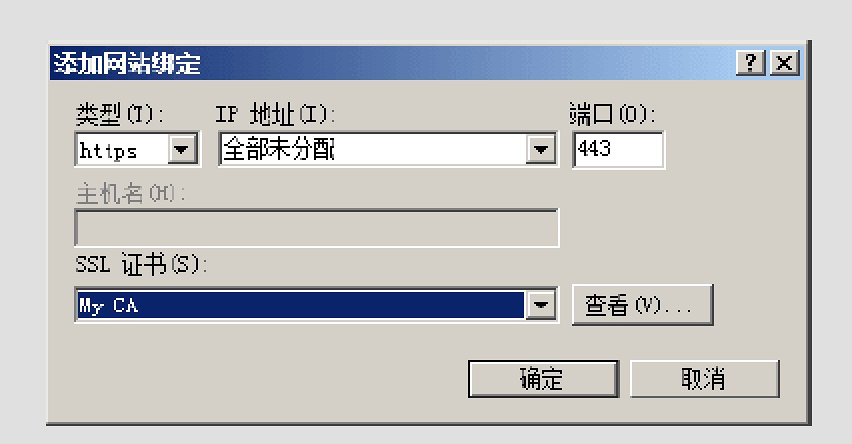
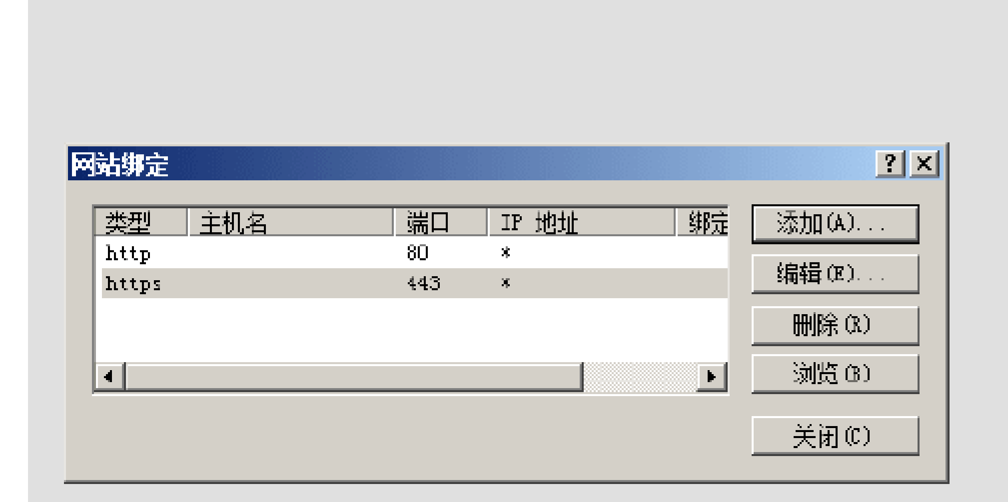


图 12-21　【网站绑定】对话框

图 12-22　【添加网站绑定】对话框

（17）在【网站绑定】对话框中，单击【关闭】按钮，如图 12-23 所示。

（18）在【Internet 信息服务（IIS）管理器】窗口中，选择 mytext 选项，并在右侧 IIS 区域中，双击【SSL 设置】图标，如图 12-24 所示。



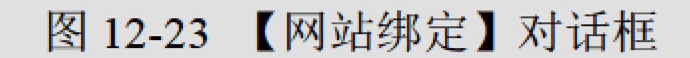

图 12-23 【网站绑定】对话框



图 12-24 【Internet 信息服务（IIS）管理器】窗口

（19）在显示的【SSL 设置】区域中，启用【要求 SSL】复选框，并选择右侧的【应用】选项，如图 12-25 所示。

（20）在浏览器地址栏中，输入http://127.0.0.1，并按回车键，查看结果如图 12-26 所示。



图 12-25 SSL 设置



图 12-26 使用 http 方式访问

（21）在浏览器地址栏中，输入https://127.0.0.1，并按回车键，查看结果如图 12-27 所示。



图 12-27 使用 https 方式访问

第13章 数据加密及备份

随着电子商务的应用越来越多，数据的安全问题越来越受到重视。解决这一问题的关键是要对数据本身实施加密及备份，即使数据不幸泄露或丢失，也难以被人破译，且能够及时利用数据恢复工具（如 FinalData、EasyRecovery 等）进行恢复。

对数据库中数据加密及备份，是为增强普通关系数据库管理系统的安全性，提供一个安全适用的数据库加密和备份平台，对数据库存储的内容实施有效保护。它通过数据库加密、备份存储等安全方法实现了数据库数据存储保密和完整性要求，使得数据库以密文方式存储，确保数据安全。

本章主要对当前密钥加密算法（如 DES、RSA、Hash）、数据加密技术的应用、数据及数据库的备份等内容作详细的介绍。

本章学习要点：

- 密钥密码学介绍
- 数据加密技术
- 数据及数据库备份
- 数据恢复工具

13.1 密钥密码学介绍

密钥密码学是一门古老而深奥的学科，对一般人来说却是非常陌生的。长期以来，只在很小的范围内使用，如军事、外交、情报等部门。计算机密码学是研究计算机信息加密、解密及其变换的技术，是数学和计算机的交叉学科，同时也是一门新兴的学科。随着计算机网络和计算机通信技术的发展，计算机密码学得到迅速普及。在国外，已经成为计算机安全主要研究方向。

13.1.1 背景知识概述

密码学的历史比较悠久，在 4000 年前，古埃及人就开始使用密码来传递消息。2000 年前，罗马国王 Julius Caesare（恺撒）就开始使用目前称为“恺撒密码”的密码系统。但是，密码技术直到 20 世纪 40 年代以后才有重大突破和发展。特别是 20 世纪 70 年代后期，由于计算机、电子通信的广泛使用，现代密码学得到了空前的发展。

与密码学相关的学科大致分为 3 个方面。其中，密码学（Cryptology）是研究信息系统安

全保密的科学；密码编码学（Cryptography）主要研究对信息进行编码，实现对信息的隐藏；密码分析学（Cryptanalytis）主要研究加密消息的破译或消息的伪造。密码学的发展大致经过3个阶段。

第一阶段是1949年之前，密码学是一门艺术，这个阶段的研究特点如下所述。

- ❑ 密码学不是科学，而是艺术。
- ❑ 出现一些密码算法和加密设备。
- ❑ 密码算法的基本手段出现，主要针对字符。
- ❑ 简单的密码分析手段出现，数据的安全基于算法的保密。

该阶段具有代表性事件是1883年Kerchoffs第一次明确地提出了编码原则，即加密算法应建立在算法的公开而不影响明文和密钥的安全上。这个原则得到广泛承认，成为判定密码强度的衡量标准，实际上也成为传统密码和现代密码的分界线。

第二阶段是1949～1975年，密码学成为一门独立的科学，该阶段计算机的出现使基于复杂计算机的密码成为可能。主要研究特点是数据安全基于密钥而不是算法的保密。

第三阶段是1976年以后，密码学中公钥学成为主要研究方向，该阶段具有代表性的事件如下所述。

- ❑ 1976年，Diffie和Hellman提出了不对称密钥。
- ❑ 1977年，Rivest、Shamir和Adleman提出了RSA（Rivest Shamir Adleman）公钥算法。
- ❑ 1977年，DES（Data Encryption Standard）算法出现。
- ❑ 20世纪80年代，出现IDEA和CAST等算法。
- ❑ 20世纪90年代，对称密钥算法进一步成熟，逐步出现了Rijindael，RC6和椭圆曲线等其他公钥算法。
- ❑ 2001年，Rijindael成为DES算法的替代者。
- ❑ 2004年8月，山东大学信息安全所所长在国际会议上，首次宣布了她及她的研究小组对MD5、HAVAL-128、MD4和RIPEMD这4个著名密码算法的破译结果。

这个阶段的主要特点是公钥使得发送端和接收端无密钥传输的保密通信成为可能。

13.1.2　密钥密码学简介

计算机网络的广泛应用，产生了大量的电子数据，这些电子数据需要传输到网络的许多地方。有意的计算机犯罪和无意的数据破坏对这些数据产生了很大的威胁。国家机密、企业经济信息、银行网上业务等的任何差错都会使国家安全、企业经营受到巨大的损害。从原则上来说，对电子数据的攻击有两种形式。

- ❑ **被动攻击**　即非法从传输信道上截取信息，或从存储载体上偷窃信息。
- ❑ **主动攻击**　即对传输或存储的数据进行恶意的删除、修改等。

虽然对这些行为已经建立相应的法律，但由于这种犯罪形式的特殊性，对于它的监督很困难。因此，在不断完善相应法律和监督的同时，还需要加强自我保护，密钥密码技术是一种有效而经济的方法。

密钥密码学是关于加密和解密的理论，主要用于保密通信。目前，密码学已经得到了更加深入、广泛的发展，其内容已不再是单一的加解密技术，已被有效、系统地用于保证电子

数据的保密性、完整性和真实性。保密性就是对数据进行加密，使非法用户无法读懂数据信息，而合法用户可以应用密钥读取信息。完整性是对数据完整性的鉴别，以确定数据是否被非法篡改，保证合法用户得到正确、完整的信息。真实性是数据来源的真实性、数据本身真实性的鉴别，可以保证合法用户不被欺骗。

现代密钥密码技术的应用，已经深入到数据处理过程的各个环节，包括数据加密、密码分析、数据签名、信息鉴别、秘密共享等。密钥密码学的数学工具也更加广泛，有概率统计、数论、代数等。

13.1.3　当前密钥加密算法

据不完全统计，到现在为止，已经公开发表的各种加密算法多达数百种。但针对于目前常见的加密算法大体分成三类：对称加密算法，非对称加密算法和 Hash 算法。

1. 对称加密算法

对称算法就是加密密钥能够从解密密钥中推算出来，反过来也成立。大多数对称算法中，加、解密的密钥是相同的，这些算法也称为保密密钥算法或单密钥算法。它要求发送者和接收者在安全通信之前，商定一个密钥。算法的安全性依赖于密钥，只要通信需要保密，密钥就必须保密。

对称算法又分为分组算法和序列算法两类，两者的区别在于分组算法是对一个大的明文数据块（分组）进行运算；序列算法是对明文中单个位（或字节）进行运算。对称算法体制的发展趋势，将以分组密码为重点。著名的对称密码算法有 DES、3DES、Blowfish、IDEA、RC4、RC5、RC6 和 AES。

❑ **DES 数据加密标准**

最著名的保密密钥或对称密钥加密算法 DES（Data Encryption Standard），是由 IBM 公司在 20 世纪 70 年代发展起来的，该标准于 1977 年由美国国家标准局颁布，主要用于用户敏感信息的保护，后被国际标准化组织接受作为国际标准。DES 主要采用替换和移位的方法，使用 56 位密钥每次处理 64 位数据，运算速度快，易于用软件实现，也适合在专用芯片上实现。

DES 是一种世界公认的优秀加密算法，自问世以来经历了许多科学家的研究和破译，曾为全球贸易、金融等部门提供可靠的通信安全保障。但它也有明显的缺点：密钥太短，只有 56 位。目前已有许多 DES 被破译的报道，因此为了提高安全性，DES 又有了新的发展。例如，三重 DES 使用双密钥加密的方法，即使用两个 56 位的密钥 k1、k2，发送方用 k1 加密，k2 解密，再使用 k1 加密。接收方则使用 k1 解密，k2 加密，再使用 k1 解密，其效果相当于将密钥的长度增加到 112 位。还有三重 DES 的变形算法 IDEA，使用 3 个独立密钥，相当于密钥长度增加到 168 位。

❑ **IDEA 国际数据加密算法**

IDEA（International Data Encryption Algorithm）由瑞士的 Xuejia Lai 和 James Massey 于 1990 年正式公布，并在以后得到增强。这种算法是在 DES 算法的基础上发展起来的，类似于三重 DES。IDEA 的产生，同样是因为 DES 使用的密钥太短。IDEA 的密钥为 128 位，这么长的密钥在未来若干年内应该是安全的。

IDEA 算法也基于分组，它采用软件和硬件实现都同样快速，且目前软件实现的 IDEA 比 DES 快两倍。由于 IDEA 是在美国之外提出并发展起来的，避开了美国法律上对加密技术的诸多限制。因此，有关 IDEA 算法和实现技术的资料可以自由出版和交流，极大地促进 IDEA 的发展和完善。但由于该算法是一个相对较新的算法，针对它的攻击也还不多，还未经过较长时间的考验。因此，尚不能判断出它的问题和缺陷。

这一类算法的优点是有很强的保密强度，且经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。

2. 公开密钥算法

公开密钥算法是指使用一对密钥加解密信息，加密的密钥不同于解密的密钥，而且解密的密钥不能根据密钥在合理的时间和财力内计算出来。之所以叫公开密钥算法（公钥算法），是因为加密密钥能够公开，任何人都可以使用加密密钥加密信息，但只有用相应的解密密钥才能解密信息。

常见的非对称加密算法有 RSA、ECC（移动设备用）、Diffie-Hellman、椭圆曲线、DSA（数字签名用）等。

- **RSA 算法**

RSA 由美国的 Rivest、Shamir 和 Adleman 于 1978 年提出。该算法基于大数分解的难度，即已知较大合数 n，求 pq，使 n=pq。所以，随着大整数分解算法和计算能力的不断提高，对 RSA 的破译能力也在增强。有报道 482 位的 RSA 已被利用数域 NFS 分解出来，512 位也可以在数月时间内被分解，1024 位的 RSA 目前仍是比较安全的。与 DES 相比，RSA 拥有更高的安全，但执行速度慢，因此两者经常结合起来使用，DES 加密速度快，适合加密较长的报文；而 RSA 可解决 DES 密钥分配的问题。

例如，用户 A 要与用户 B 通信，首先 A 产生一个与 B 通信的 DES 密钥，用 B 的公钥对通信密钥加密后传给 B，B 用其私有密钥（只有 B 拥有）解密，获得双方的一次性通信 DES 密钥。然后双方采用此 DES 通信进行保密通信。

- **Diffe-Hellman 算法**

该算法是第一个公钥算法，由美国的 Diffe 和 Hellman 于 1976 年提出。其安全性源于在有限域上计算离散对数比计算指数更困难，该算法主要用于密钥交换。协议如下：首先 A 与 B 协商两个大的素数 n 和 g；然后，A 选取一个大的随机数 x 并且发送给 B，X＝gx mod n；B 选取一个大的随机数 y 并且发送给 A，Y＝gy mod n；A 计算 k2＝Yx mod n；B 计算 k2＝Xy mod n，k1 和 k2 都等于 gxy mod n，偷听者即使知道 n，g，X 和 Y，也无法计算出 k，除非他们计算离散对数，因此 k 是 A 与 B 的秘密密钥。

- **椭圆曲线**

椭圆曲线已研究了许多年，Koblitz 和 Miller 于 1985 年分别提出将它用于公钥密码体制。椭圆曲线的引人之处，在于提供了由元素和组合规则来组成群的构造方法，即利用椭圆曲线上的点构成 Abelian 加法群构造离散对数问题。基于有限域 GF（2n）的椭圆曲线算术运算器很容易构造，并且 n 在 130 位至 200 位之间的实现相当简单，它提供了一个更快且具有更小密钥长度的公钥算法。

公钥密码的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方

便地实现数字签名和验证。但其算法复杂，加密数据的速率较低。尽管如此，随着现代电子技术和密码技术的发展，公钥密码算法将是一种很有前途的网络安全加密体制。

当然在实际应用中，人们通常将对称密码和公钥密码结合在一起使用。例如，利用 DES 或者 IDEA 来加密信息，而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特来分类，可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特而后者则先将信息序列分组，每次处理一个组。

3. Hash 算法

Hash 算法特别之处在于它是一种单向算法，用户可以通过 Hash 算法对目标信息生成一段特定长度的唯一的 Hash 值，却不能通过这个 Hash 值重新获得目标信息。因此 Hash 算法常用于不可还原的密码存储、信息完整性校验等。常见的算法有 MD2、MD4、MD5、HAVAL、SHA。加密算法的效能通常可以按照算法本身的复杂程度、密钥长度（密钥越长越安全）、加解密速度等来衡量。上述的算法中，除了 DES 密钥长度不够、MD2 速度较慢已逐渐被淘汰外，其他算法仍在目前的加密系统产品中使用。

例如，MD5（Message-Digest Algorithm 5）是在 20 世纪 90 年代初由 MIT（Massachusetts Institute of Technology，美国麻省理工学院）的计算机科学实验室和 RSA Data Security Inc 公司发明，经 MD2、MD3 和 MD4 发展而来。

Message-Digest 泛指字节串（Message）的 Hash 变换，就是把一个任意长度的字节串变换成一定长的大整数。需要注意这里使用的“字节串”与“字符串”不属于同一个概念，因为这种变换只与字节的值有关，而与字符集或编码方式无关。

MD5 将任意长度的“字节串”变换成一个 128bit 的大整数，并且它是一个不可逆的字符串变换算法，换句话说，即使看到源程序和算法描述，也无法将一个 MD5 的值变换回原始的字符串，从数学原理上说，是因为原始的字符串有无穷多个，这类似于不存在反函数的数学函数。

MD5 的典型应用是对一段 Message（字节串）产生 fingerprint（指纹），以防止被“篡改”。例如，将一段话写在名为 readme.txt 文件中，并对这个 readme.txt 产生一个 MD5 的值并记录在案，然后将这个文件传送给其他人，如果该接收者修改了文件中的任何内容，那么当再次对这个文件重新计算 MD5 时就会被发现。如果存在第三方的认证机构，同样也可用 MD5 防止文件作者的“抵赖”，这就是所谓的数字签名应用。

MD5 还广泛用于加密和解密技术上。在很多操作系统中，用户的密码是以 MD5 值（或类似的其他算法）方式保存的，当用户登录时，系统会将用户输入的密码计算成 MD5 值，然后再去和系统中保存的 MD5 值进行比较，而系统并不“知道”用户的密码是什么。

一些黑客破获这种密码的方法是一种被称为“跑字典”的方法，先用 MD5 程序计算出这些字典项的 MD5 值，然后再用目标的 MD5 值在这个字典中检索。目前，有两种方法可以得到字典，一种是日常搜集用作密码的字符串表，另一种是用排列组合方法生成的。

即使密码的最大长度为 8，同时密码只能是字母和数字，共 26+26+10=62 个字符，排列组合出的字典的项数则是 P(62,1)+P(62,2)+…+P(62,8)，那也是一个巨大的数字，存储这个字典就需要 TB 级的磁盘组，而且这种方法还有一个前提，就是能获得目标账户的密码 MD5 值。

另外，在很多电子商务和社区应用中，管理用户记录（Account）是一种最常用的基本功

能，尽管许多应用服务器（Application Server）提供了这些基本组件，但很多应用开发者为了管理的更大的灵活性还是喜欢采用关系数据库来管理用户，懒惰的做法是用户的密码往往使用明文或简单的变换后直接保存在数据库中。因此这些用户的密码对软件开发者或系统管理员来说，毫无保密可言。这里主要介绍 MD5 的 Java Bean（可以重复使用的软件代码打包标准）的实现，这种方法使得管理员和程序设计者都无法看到用户的密码，尽管他们可以初始化这些密码。但重要的一点是对于用户密码设置习惯的保护。

13.1.4　密钥的发布和管理

密钥既然要求保密，就必须涉及密钥的管理问题，管理不好，密钥同样可能被无意识地泄露。因为任何保密也只是相对的，具有一定的时效性。要管理好密钥还要注意以下几个方面。

1. 密钥的使用要注意时效和次数

如果用户可以重复地使用同样密钥与别人交换信息，那么密钥也同其他任何密码一样存在着一定的安全性，虽然用户的私钥是不对外公开的，但也很难保证私钥一直不被泄露。如果某人偶然知道了用户的密钥，那么用户曾经和另一个人交换的每一条消息都不再是保密的。另外，使用一个特定密钥加密的信息越多，提供给窃听者的材料也就越多，从某种意义上来讲也就越不安全。

因此，一般强调仅将一个对话密钥用于一条信息中或一次对话中，或者建立一种按时更换密钥的机制以减小密钥暴露的可能性。

2. 多密钥的管理及发布

在某机构中有 100 个人，如果他们任意两人之间可以进行秘密对话，那么总共需要多少密钥呢？每个人需要知道多少密钥呢？也许很容易得出答案，如果任何两个人之间要不同的密钥，则总共需要 4950 个密钥，而且每个人应记住 99 个密钥。如果机构的人数是 1000、10000 人或更多，这种办法显然不合适（对密钥的管理将是一件可怕的事情）。

Kerberos 提供了一种解决这个问题的较好方案，由 MIT 发明的，使保密密钥的管理和分发变得十分容易，但这种方法本身还存在一定的缺点。为能在因特网上提供一个实用的解决方案，Kerberos 建立了一个安全的、可信任的密钥分发中心（Key Distribution Center，KDC），每个用户只要知道一个和 KDC 进行会话的密钥就可以了，而不需要知道成百上千个不同的密钥。

假设用户甲想要和用户乙进行秘密通信，则用户甲先和 KDC 通信，用只有用户甲和 KDC 知道的密钥进行加密，用户甲告诉 KDC 希望和用户乙进行通信，KDC 会为用户甲和用户乙之间的会话随机选择一个对话密钥，并生成一个标签，这个标签由 KDC 和用户乙之间的密钥进行加密，并在用户甲启动和用户乙对话时，用户甲会把这个标签交给用户乙。这个标签的作用是让用户甲确信和他交谈的是用户乙，而不是冒充者。因为这个标签是由只有用户乙和 KDC 知道的密钥进行加密的，所以即使冒充者得到用户甲发出的标签也不可能进行解密，只有用户乙收到后才能进行解密，从而确定了与用户甲对话的人就是用户乙。

当 KDC 生成标签和随机会话密码，就会把它们用只有用户甲和 KDC 知道的密钥进行加密，然后把标签和会话密钥传给用户甲，加密的结果可以确保只有用户甲能得到这个信息，且只有用户甲能利用这个会话密钥和用户乙进行通话。同理，KDC 会把会话密码用只有 KDC 和用户乙知道的密钥加密，并把会话密钥给用户乙。

用户甲会启动一个和用户乙的会话，并用得到的会话密钥加密自己和用户乙的会话，还要把 KDC 传给它的标签传给用户乙以确定用户乙的身份，然后用户甲和用户乙之间就可以用会话密钥进行安全的会话了，而且为了保证安全，这个会话密钥是一次性的，这样黑客就更难进行破解了。同时由于密钥是一次性由系统自动产生的，则用户不必记那么多密钥，方便了人们的通信。

13.2　数据加密技术

网络安全是一个系统的概念，完善的网络安全体系，必须合理协调法律、技术和管理这 3 个因素。主要表现在保密、访问控制、身份认证、不可否认和完整性方面。其中数据保密是首要的，数据不能被非法用户访问。身份认证是由于通信双方不在一起，因此数据传输前需确认对方的身份是真实可信的。完整性指用户从网上获得的信息未被篡改过，针对上述网络安全的各个方面，一些安全技术相应产生并应用，其中使用最为广泛的就是数据加密技术。

13.2.1　数据加密概述

数据加密（Data Encryption）技术是指将一个信息（或称明文，plain text）经过加密钥匙（Encryption key）及加密函数转换，转换为无意义的密文（cipher text），而接收方则将此密文经过解密函数、解密钥匙（Decryption key）还原成明文。它是网络安全技术的基石。

1．数据加密理由

当今网络社会选择数据加密已是别无选择，一方面由于在互联网上进行文件传输、电子邮件商务往来存在许多不安全因素，特别是对于一些大公司和一些机密文件在网络上传输。而且这种不安全性是互联网存在基础——TCP/IP 协议所固有的，包括一些基于 TCP/IP 的服务。另一方面，互联网给众多的商家带来了无限的商机，互联网把全世界连在了一起，走向互联网就意味着走向了世界，这对于无数商家无疑是件好事，特别是对于中小企业。为了解决这一矛盾，能在安全的基础上打开通向世界之门，只好选择数据加密和基于加密技术的数字签名。

加密在网络上的作用就是防止有用或私有化信息在网络上被拦截和窃取如密码的传输。计算机密码极为重要，因为许多安全防护体系是基于密码的，密码的泄露在某种意义上来讲意味着其安全体系的全面崩溃。

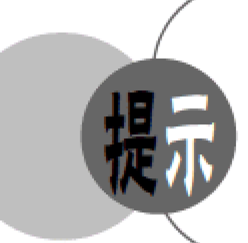
通过网络进行登录时，所键入的密码以明文的形式被传输到服务器，而网络上的窃听是一件极为容易的事情，所以用户的密码很有可能被黑客窃取，如果用户是 Root（Linux 管理员）或 Administrator（Windows 管理员），这样该系统将存在被暴露的威胁。

另外，如果公司在进行某个招标项目的投标工作，工作人员通过电子邮件的方式把单位的标书发给招标单位，此时有另一位竞争对手从网络上窃取到该公司的标书，从而知道这个公司投标的标的，那么后果将非常严重。

解决上述难题的方案就是加密，加密后的口令即使被黑客获得也是不可读的，加密后的标书没有收件人的私钥也就无法解开，标书成为一大堆无任何实际意义的乱码。总之无论是单位还是个人在某种意义上来说加密也成为当今网络社会进行文件或邮件安全传输的时代象征。

数字签名就是基于加密技术的，它的作用就是用来确定用户是否是真实的。应用最多的还是电子邮件，当用户收到一封电子邮件时，邮件上面标有发信人的姓名和信箱地址，很多人可能会简单地认为发信人就是信上说明的那个人，但实际上伪造一封电子邮件对于一个通常人来说是极为容易的事。在这种情况下，就要用到加密技术基础上的数字签名，用它来确认发信人身份的真实性。

类似数字签名技术的还有一种身份认证技术，有些站点提供入站 FTP 和 Web 服务，当然用户通常接触的这类服务是匿名服务，用户的权力要受到限制，但也有的这类服务不是匿名的，如某公司为了信息交流提供用户的合作伙伴非匿名的 FTP 服务，或开发小组把他们的 Web 网页上载到用户的 Web 服务器上，现在的问题就是，用户如何确定正在访问用户服务器的人就是用户认为的那个人，身份认证技术就是一个好的解决方案。



文件加密不只用于电子邮件或网络上的文件传输，其实也可用于静态的文件保护，如 PIP 软件就可以对磁盘、硬盘中的文件或文件夹进行加密，以防他人窃取其中的信息。

2. 数据加密方法

数据加密技术要求只有在指定的用户或网络下，才能解除密码而获得原来的数据，这就需要给数据发送方和接受方一些特殊的信息用于加解密，这就是所谓的密钥。其密钥的值是从大量的随机数中选取的。按加密算法分为专用密钥和公开密钥两种。

- **专用密钥**

专用密钥又称为对称密钥或单密钥，加密和解密时使用同一个密钥，即同一个算法。如 DES 和 MIT 的 Kerberos 算法。单密钥是最简单方式，通信双方必须交换彼此密钥，当需给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。当一个文本要加密传送时，该文本用密钥加密构成密文，密文在信道上传送，收到密文后用同一个密钥将密文解出来，形成普通文体供阅读。在对称密钥中，密钥的管理极为重要，一旦密钥丢失，密文将无密可保。这种方式在与多方通信时因为需要保存很多密钥而变得很复杂，而且密钥本身的安全就是一个问题。

对称密钥是最古老的，一般所说的“密电码”采用的就是对称密钥。由于对称密钥运算量小、速度快、安全强度高，因而目前仍被广泛采用。

- **公开密钥**

公开密钥又称非对称密钥，加密和解密时使用不同的密钥，即不同的算法，虽然两者之

间存在一定的关系，但不可能轻易地从一个推导出另一个。有一把公用的加密密钥，有多把解密密钥，如 RSA 算法。

非对称密钥由于两个密钥（加密密钥和解密密钥）各不相同，因而可以将一个密钥公开，而将另一个密钥保密，同样可以起到加密的作用。

在这种编码过程中，一个密码用来加密消息，而另一个密码用来解密消息。在两个密钥中有一种关系，通常是数学关系。公钥和私钥都是一组十分长的、数字上相关的素数（是另一个大数字的因数）。有一个密钥不足以翻译出消息，因为用一个密钥加密的消息只能用另一个密钥才能解密。每个用户可以得到唯一的一对密钥，一个是公开的，另一个是保密的。公共密钥保存在公共区域，可在用户中传递，甚至可印在报纸上面。而私钥必须存放在安全保密的地方。任何人都可以有公钥，但是只有自己才能有私钥。

公开密钥的加密机制虽提供了良好的保密性，但难以鉴别发送者，即任何得到公开密钥的人都可以生成和发送报文。数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充和篡改等问题。

当然在实际应用中人们通常将两者结合在一起使用。即利用 DES 或者 IDEA 来加密信息，而采用 RSA 来传递会话密钥。

密码技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。

13.2.2　数据加密应用

数据加密可以使人们在因特网上进行安全的会话，而不必担心会被人偷听。随处可见的虚拟局域网（VPN）、最新的加密和鉴别（数字签名）技术都是很好的数据加密技术的应用。

1. 在电子商务方面的应用

电子商务（E-business）要求顾客可以在网上进行各种商务活动，不必担心自己的信用卡会被人盗用。在过去，用户为了防止信用卡的号码被窃取到，一般是通过电话订货，然后使用用户的信用卡进行付款。现在人们开始用 RSA（一种公开/私有密钥）的加密技术，提高信用卡交易的安全性，从而使电子商务走向实用成为可能。

许多人都知道网景通讯（Netscape）公司是 Internet 商业中领先技术的提供者，提供了一种基于 RSA 和保密密钥应用于因特网的技术，被称为安全插座层（Secure Sockets Layer，SSL）。

另外，还有 Socket 程序。它只是一个编程界面，不提供任何安全措施，而 SSL（安全套接字）不仅提供编程界面，还向上提供一种安全的服务，SSL3.0 现在已经应用于服务器和浏览器，SSL2.0 则只能应用于服务器端。

SSL3.0 用一种电子证书（electric certificate），用来进行身份验证后，双方就可以用保密密钥进行安全的会话了。它同时使用“对称”和“非对称”加密方法，在客户与电子商务的服务器进行沟通的过程中，客户会产生一个会话密钥，然后客户用服务器端的公钥将会话密钥进行加密，再传给服务器端，在双方都知道会话密钥后，传输的数据都是以会话密钥进行加密与解密的，但服务器端发给用户的公钥必须先向有关发证机关申请，以得到公证。

基于 SSL3.0 提供的安全保障，用户就可以自由订购商品并给出信用卡号，也可以在网上

和合作伙伴交流商业信息并且让供应商把订单和收货单从网上发过来，这样可以节省大量的纸张，为公司节省大量的电话、传真费用。通常，电子信息交换（Electric Data Interchange，EDI）、信息交易（Information Transaction）和金融交易（Financial Transaction）都是在专用网络上完成的，使用专用网的费用大大高于互联网。正是这样巨大的诱惑，才使人们开始发展因特网上的电子商务，但不要忘记数据加密。

2. 加密技术在 VPN 中的应用

虚拟专用网是一种基于公共数据网，给用户一种直接连接到私人局域网感觉的服务。VPN 极大地降低了用户的费用，而且提供了比传统方法更强的安全性和可靠性。

VPN 可分为三大类。

- ❑ 企业各部门与远程分支之间的 Intranet VPN。
- ❑ 企业网与远程（移动）雇员之间的远程访问（Remote Access）VPN。
- ❑ 企业与合作伙伴、客户、供应商之间的 Extranet VPN。

现在，越来越多的公司走向国际化，一个公司可能在多个国家都有办事机构或销售中心，每一个机构都有自己的局域网 LAN（Local Area Network），但在当今的网络社会人们的要求不仅如此，用户希望将这些 LAN 连结在一起组成一个公司的广域网，现在这将不再是难题。

事实上，很多公司都已经这样做了，但他们一般使用租用专用线路来连接这些局域网，他们考虑的就是网络的安全问题。现在具有加密/解密功能的路由器已到处都是，这就使人们通过互联网连接这些局域网成为可能，这就是通常所说的虚拟专用网。当数据离开发送者所在的局域网时，该数据首先被用户端连接到互联网上的路由器进行硬件加密，数据在互联网上是以加密的形式传送的，当达到目的 LAN 的路由器时，该路由器就会对数据进行解密，这样目的 LAN 中的用户就可以看到真正的信息了。

13.2.3 EFS 概述

EFS（Encrypting File System，加密文件系统）是一个由 Windows 2000 系列、Windows XP 专业版以及 Windows.NET 提供的透明的文件加密服务，以公共密钥加密为基础，使用了 Windows 中的 CryptoAPI 架构。它可以使文件具有机密性（但不提供完整保护）；提供可选的数据恢复能力，系统管理员可以恢复另一用户加密的数据；还可以实现多用户（被许可的用户）共享存取一个已经加密的数据。

1. EFS 的技术结构与原理

EFS 采用基于公钥的方案实现数据加密或解密，它使用标准 X.509 证书。每一个受保护的文件，都将被一个使用带有一定长度的文件加密密钥（FEK）的快速对称加密算法加密（FEK 的长度由算法或法则决定）。一个用户要访问一个已加密的文件，他必须拥有与公钥相适应的私钥。

❑ **加密和解密**

EFS 中，文件转换是加密和解密文件的过程，它需要一个特殊的接口。即使在严重的失败产生时，数据在转换过程中仍然是不会丢失的，所以，EFS 会备份没经过加密的原数据直

到全部转换过程都已经完成。当 EFS 接到转换文件的请求时，它首先进行一系列的检查，这些检查包括文件是否可以加密以及是否有足够的磁盘空间进行加密。系统文件或在系统目录中的文件是不能被 EFS 加密的。如果经过检查说明文件可以被加密，EFS 便产生一个文件加密密钥（FEK）。对于 FEK 加密与解密，在微软公司发布的《Windows 2000 的加密文件系统白皮书》中对 EFS 加密原理作了以下描述。

FEK 加密使用一个或多个密钥加密公钥，生成一个加密的 FEK 列表。用户密钥对的公共部分用来加密 FEK，然后将加密的 FEK 列表与加密文件一起存储在一个特殊的 EFS 属性中，该属性称为数据加密字段（DDF），把文件加密信息与文件紧密地捆绑在一起。用户密钥对的私有部分在解密过程中使用。FEK 将通过使用密钥对的私有部分（安全地存放在别的地方，如智能卡或其他安全存储设备上）进行解密的。

FEK 也使用一个或多个恢复密钥加密公钥进行加密。再者，每个密钥对的公共部分用来加密 FEK。此加密的 FEK 列表与文件一起存储在一个特殊的 EFS 属性中，该属性称为数据恢复字段（DRF）。加密 DRF 中的 FEK，只需要恢复密钥对的公共部分。在正常文件系统操作中，要求这些公共恢复密钥始终在 EFS 系统上。恢复本身一般很少用到，只是当用户离开公司或者丢失密钥时才使用。正因为如此，恢复代理可以将密钥的私有部分安全地存放到别的地方（智能卡或其他安全的存储设备上）。

然后，EFS 将在相应的文件夹建立一个临时文件。每一个源文件数据流都以备份用途被复制到这个临时文件中，源文件被缩短并且 EFS 读取这个临时文件中的数据并将它们写入原始文件，由于 EFS 加密是透明的，因而在实际写入磁盘前，EFS 便已将数据加密。当所有数据被写入原始文件以及 EFS 证明了文件已加密后，EFS 才会删除这个临时文件。如果转换失败或转换过程中发生错误，EFS 会在删除临时文件前将试图加密的文件恢复到原始状态。

❑ **打开与读写原理**

EFS 拥有打开、读、写以及转换文件 4 个主要操作。由于 EFS 被设计成透明的，对于打开、读取、写入已加密文件便与操作普通文件没有任何区别，应用程序仍然使用普通的 Win32 APIs。应用程序使用 CreateFile()或者 OpenFile()代码来打开已加密的文件；用 ReadFile()、ReadFileEx()以及 ReadFileScatter()来读取已加密的文件；用 WriteFile()、WriteFileEx()、WriteFileScatter()来写入已加密的文件。

❑ **数据恢复**

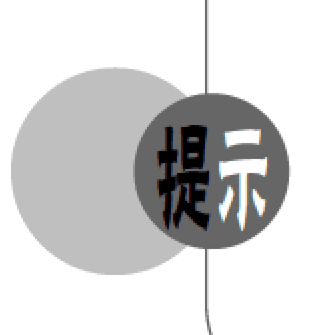
EFS 具有数据恢复能力，当用户的密钥损坏或丢失时 EFS 数据恢复便可以恢复已经加密的文件。系统管理员可以在恢复代理策略、空恢复策略以及无恢复策略中选择一种恢复策略。在域中，当设置首域控制器时，Windows 执行该域默认故障恢复策略。恢复代理策略是指系统管理员添加了一个或多个恢复代理。这些代理在管理范围中恢复任何已加密数据都是可受响应的。空恢复策略是指系统管理员删除了所有的恢复代理以及他们的公钥证书。（*EFS 不允许管理员在 Windows 2000 中选择此设置。）

无恢复策略是指系统管理员删除了恢复策略的私钥，这时没有私钥是可用的，所以不可能使用恢复代理，并且 EFS 的恢复也是不可用的。在独立的机器上，初始是没有恢复策略的，独立计算机的系统管理员可以修改 EFS 恢复策略，并且可以向恢复策略添加或创建恢复证书。

2. EFS 加密特征

与其他加密程序相比，EFS 具有以下特征。

- EFS 用户加密或解密文件或文件夹非常方便。只需用户右击要加密的文件，然后执行【加密内容以便保护数据】命令即可。
- 访问加密的文件快且容易。如果用户持有一个已加密的 NTFS 文件的私钥，那么用户能够打开这个文件，并透明地将该文件作为普通文档使用，反之，用户会被拒绝对文件的访问。而并不像第三方加密软件一样在每次存取时都要求输入密码。
- 加密后的数据无论怎样移动都保持加密状态(前提要在 NTFS 分区下移动，在 Windows 2000/XP 以及 Windows.NET 系统中，如果试图把一个 EFS 加密文件移动或复制到 FAT/FAT32 分区会遭到拒绝)。
- EFS 与 NTFS 紧密地集成在一起。当创建临时文件时，只要所有文件在 NTFS 卷上，原始文件的属性就会被复制到临时文件中。如果加密了一个文件，EFS 也会将其临时文件进行加密。EFS 驻留在操作系统内核中，并且使用不分页的池存储文件加密密钥，保证了密钥不会出现在分页文件中。这样防止了一些应用程序在创建临时文件时泄密。
- 通过 EFS 加密敏感性文件，会增加更多层级的安全性防护。在加密文件时，即使黑客已完全存取计算机的文件储存体，其文件仍然受到保护。



EFS 是为用户提供的一个内建在 Windows 产品中的方便快捷并且强大的加密系统。但同时，还设计了让其他操作系统也能读取 NTFS 的文件格式，来使用户能够避开硬盘故障以及启动分区故障。因此，使用某些操作系统可以很容易地绕过 NTFS 安全机制，存取 NTFS 文件。尽量把组织或网络中所有机器都安装 Windows 2000（或以上）的操作系统，所有分区都格式化成 NTFS，这样可以提高安全性以及避免敏感数据遭受袭击的可能性。

13.3 操作实例一

13.3.1 操作实例——使用 EFS 加密文件或文件夹

加密文件系统是 Windows 2000/XP/Vista/Server 2003/Server 2008 所特有的一个实用功能，对于 NTFS 卷上的文件和数据，都可以直接加密保存，在很大程度上提高了数据的安全性。

1. 实例目的

- 启用 EFS 加密数据。
- 保证数据安全性。
- 验证数据安全性。

2. 实例步骤

（1）在桌面双击【我的电脑】图标，在弹出的窗口中双击【本地磁盘（C:）】图标，双击 shenglin 文件夹，右击执行【新建】|【文本文档】命令，如图 13-1 所示。

（2）在【本地磁盘（C:）】根目录中，右击 shenglin 文件夹，执行【属性】命令，在弹出的对话框中单击【高级】按钮，如图 13-2 所示。

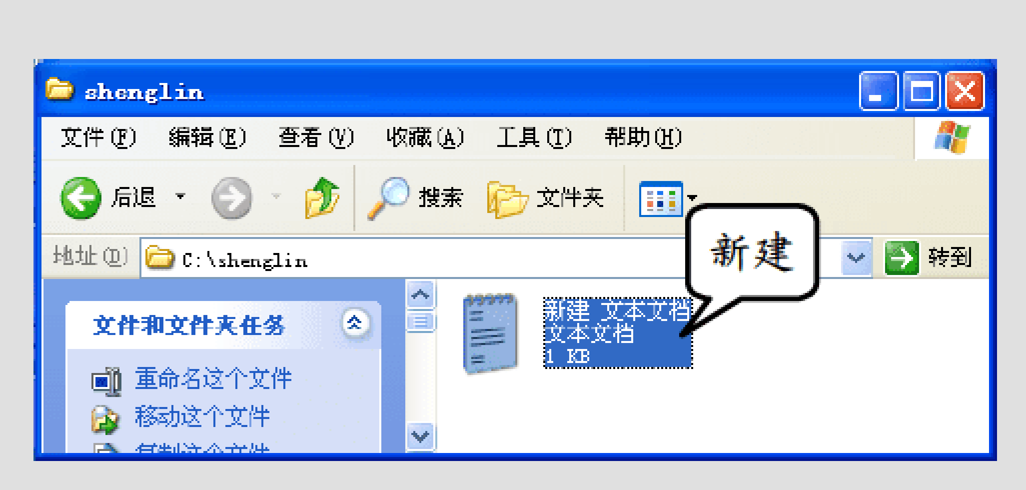


图 13-1　新建文本文档

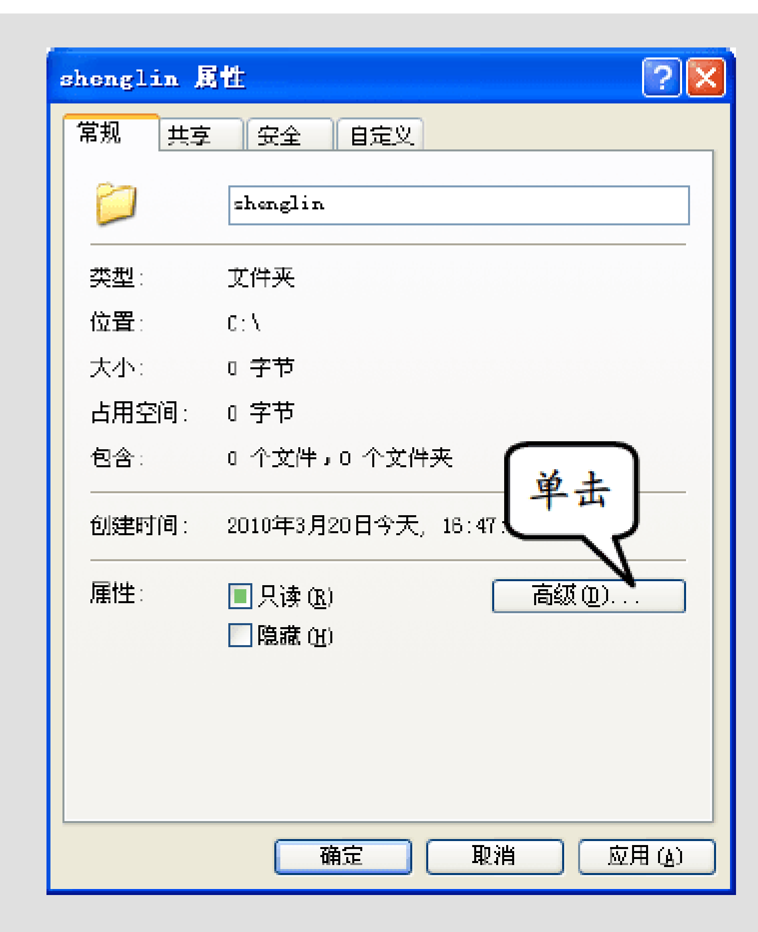


图 13-2　属性对话框

（3）在【高级属性】对话框中，启用【加密内容以便保护数据】复选框，单击【确定】按钮，如图 13-3 所示。



只有在 NTFS 分区才能进行 EFS 加密。

（4）在【shenglin 属性】对话框中，单击【应用】按钮，如图 13-4 所示。

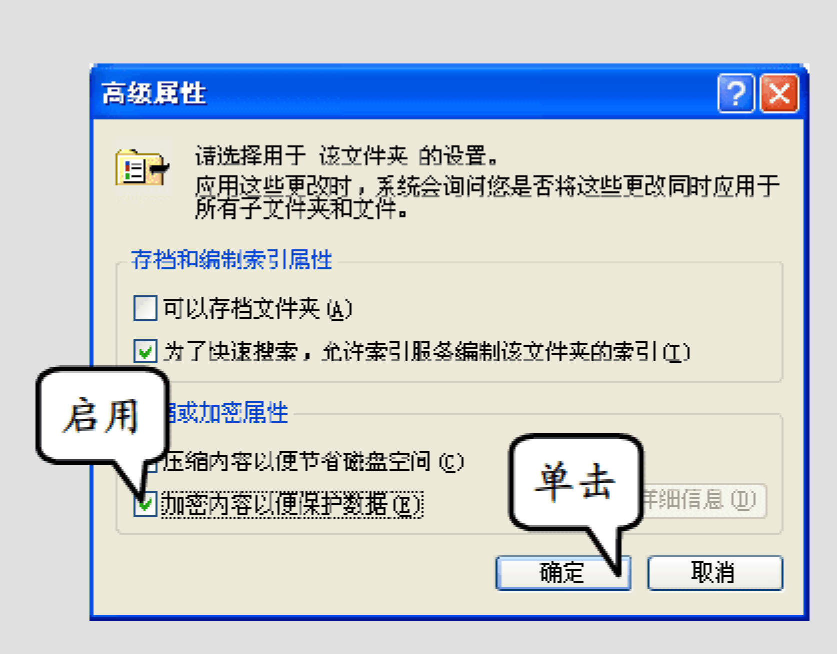


图 13-3　启用 EFS 加密

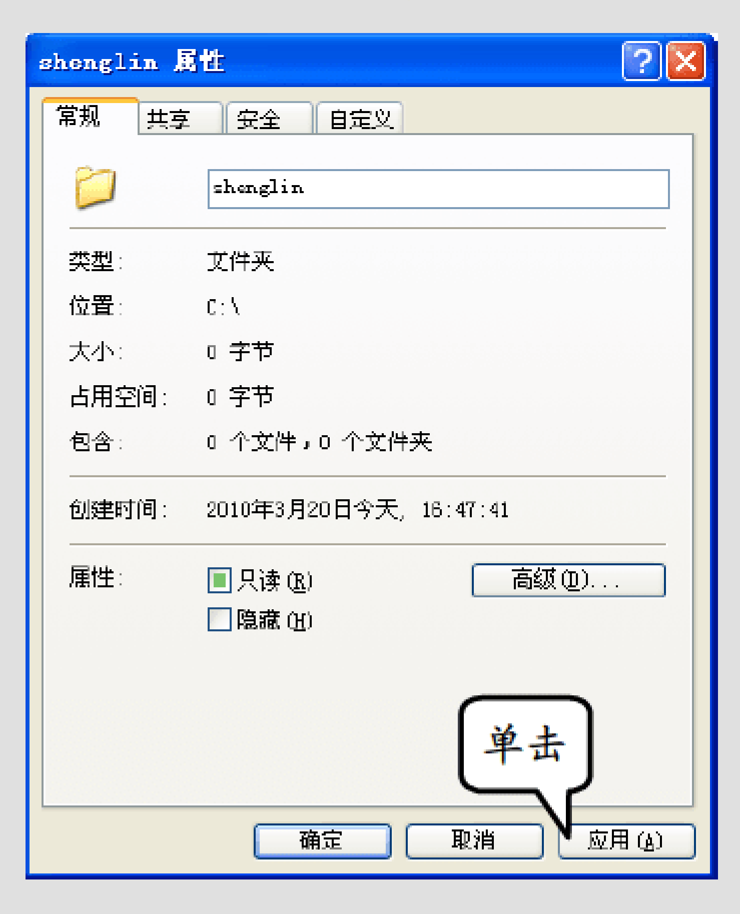


图 13-4　应用 EFS 加密

（5）在弹出的对话框中，选中【将更改应用于该文件夹、子文件和文件】单选按钮，单击【确定】按钮，如图 13-5 所示。

（6）在【本地磁盘（C:）】根目录中，可以查看到已加密的文件夹（文件名呈绿色），如图 13-6 所示。

（7）执行【开始】|【注销 administrator】命令，并在弹出的对话框中单击【注销】按钮，如图 13-7 所示。

（8）在 Windows 登录界面中，输入用户名和密码，并单击【确定】按钮，如图 13-8 所示。

（9）在【本地磁盘（C:）】根目录中，双击 shenglin 文件夹并双击【新建 文本文档】文

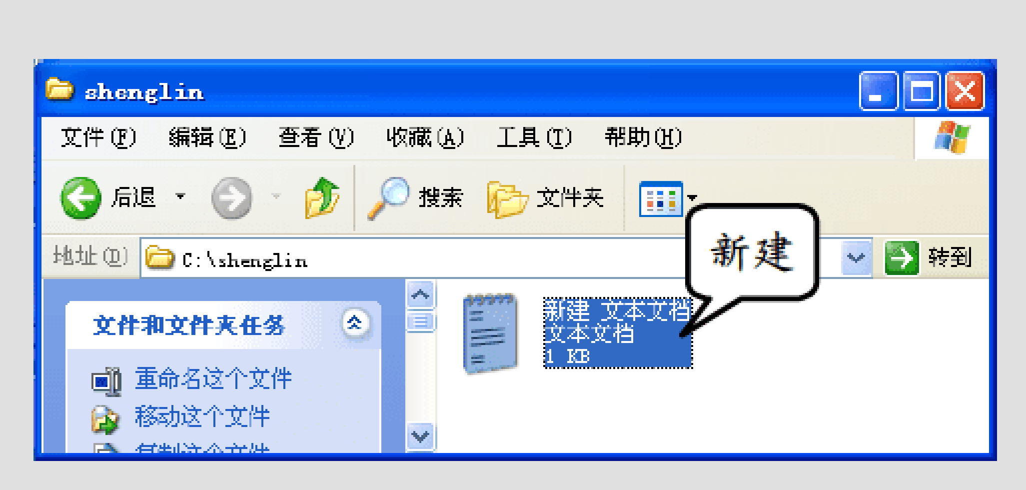


图 13-1　新建文本文档

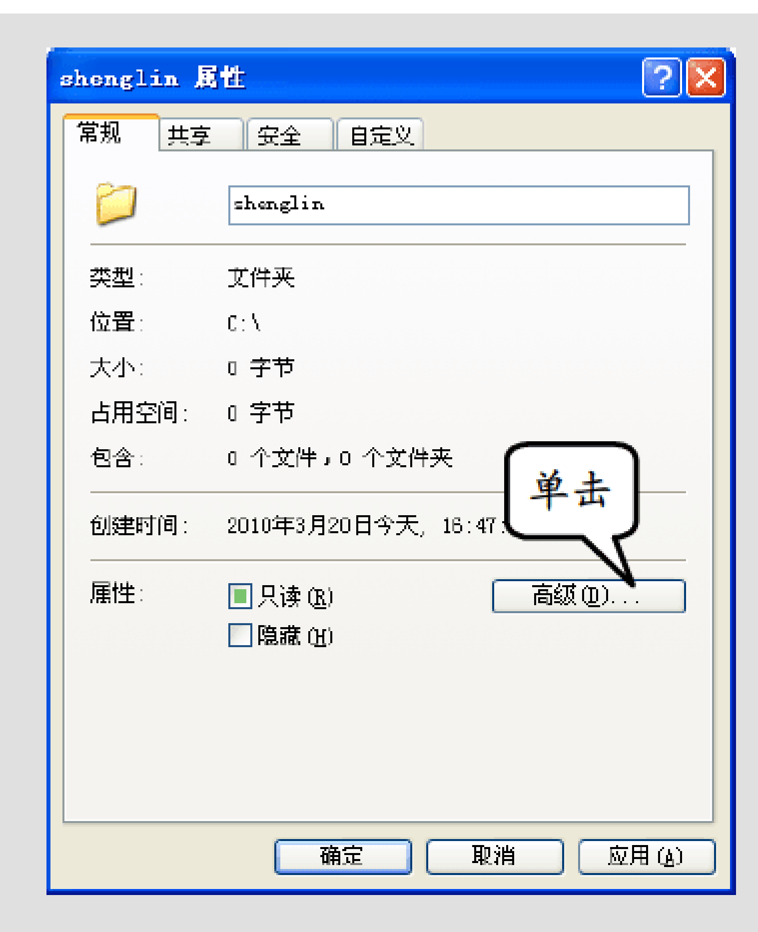


图 13-2　属性对话框

（3）在【高级属性】对话框中，启用【加密内容以便保护数据】复选框，单击【确定】按钮，如图 13-3 所示。



只有在 NTFS 分区才能进行 EFS 加密。

（4）在【shenglin 属性】对话框中，单击【应用】按钮，如图 13-4 所示。

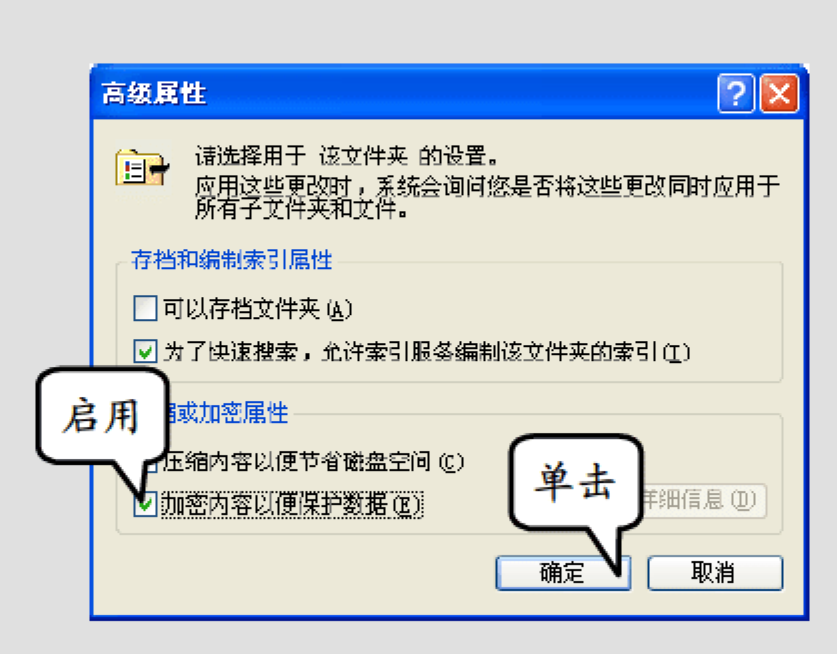


图 13-3　启用 EFS 加密

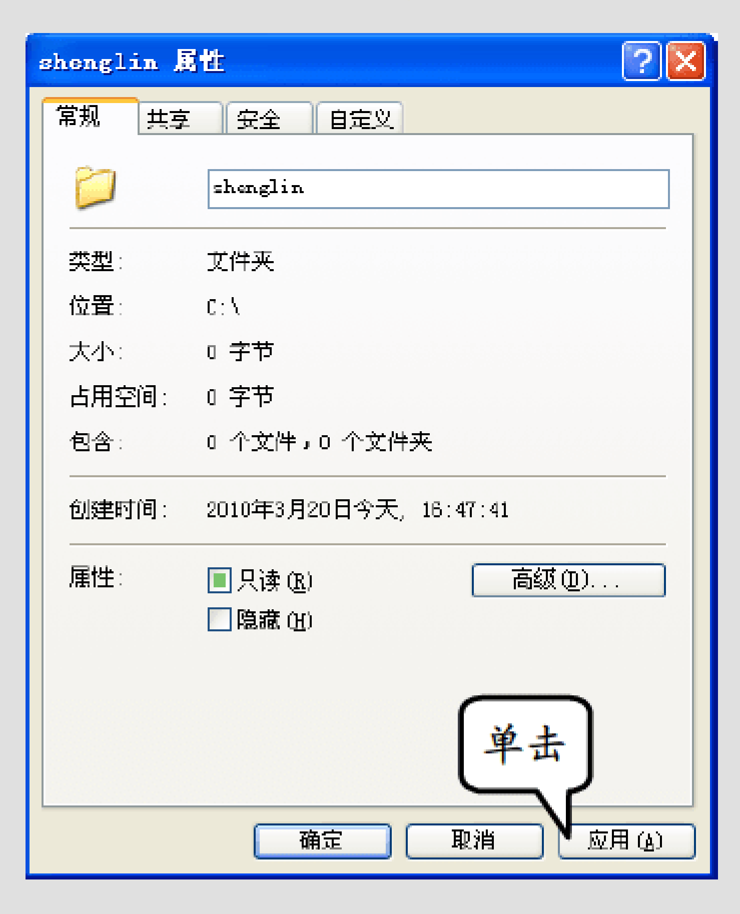


图 13-4　应用 EFS 加密

（5）在弹出的对话框中，选中【将更改应用于该文件夹、子文件夹和文件】单选按钮，单击【确定】按钮，如图 13-5 所示。

（6）在【本地磁盘（C:）】根目录中，可以查看到已加密的文件夹（文件名呈绿色），如图 13-6 所示。

（7）执行【开始】|【注销 administrator】命令，并在弹出的对话框中单击【注销】按钮，如图 13-7 所示。

（8）在 Windows 登录界面中，输入用户名和密码，并单击【确定】按钮，如图 13-8 所示。

（9）在【本地磁盘（C:）】根目录中，双击 shenglin 文件夹并双击【新建 文本文档】文

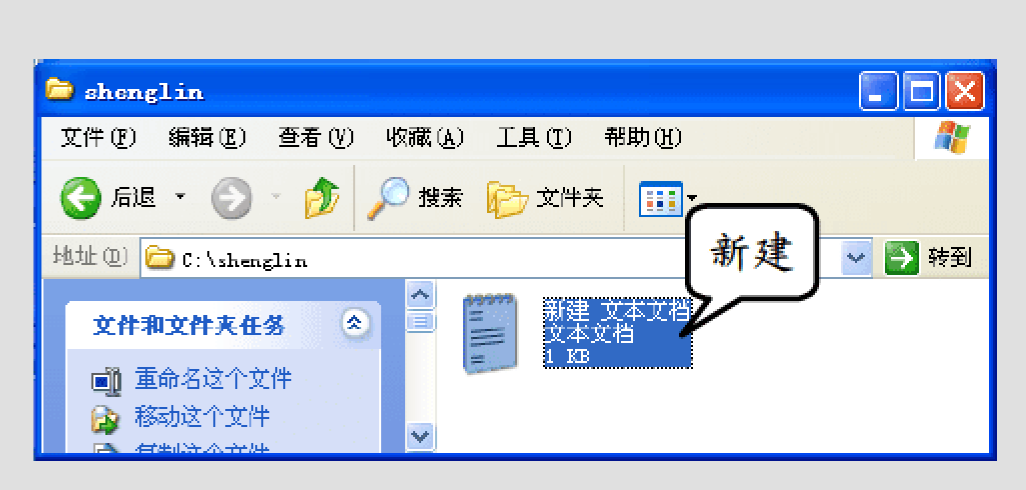


图 13-1　新建文本文档

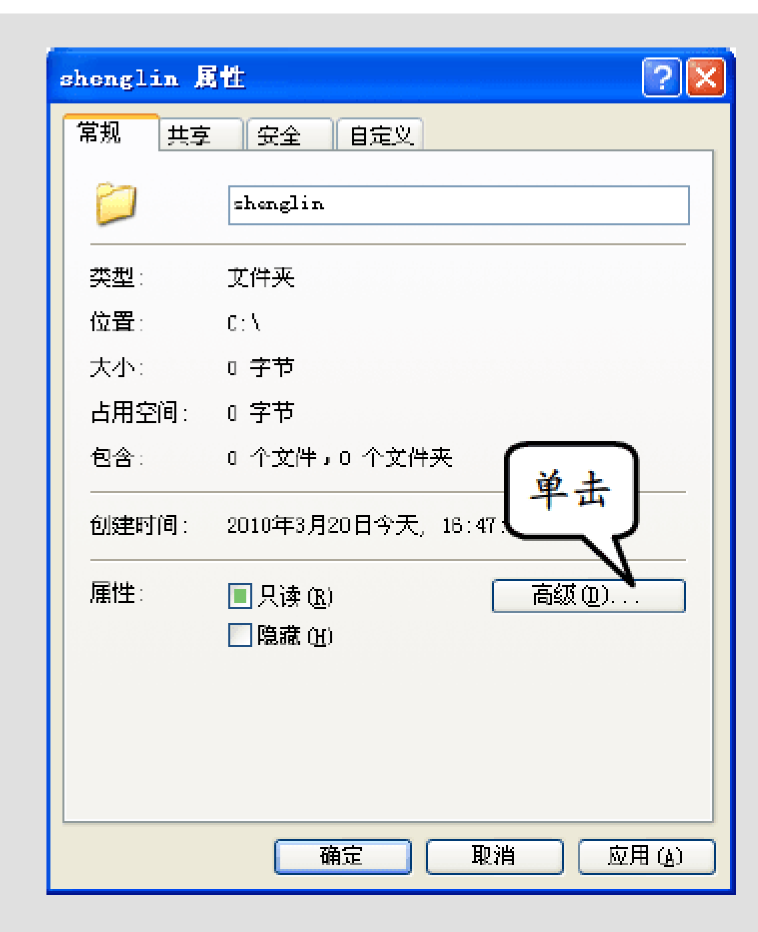


图 13-2　属性对话框

（3）在【高级属性】对话框中，启用【加密内容以便保护数据】复选框，单击【确定】按钮，如图 13-3 所示。



只有在 NTFS 分区才能进行 EFS 加密。

（4）在【shenglin 属性】对话框中，单击【应用】按钮，如图 13-4 所示。

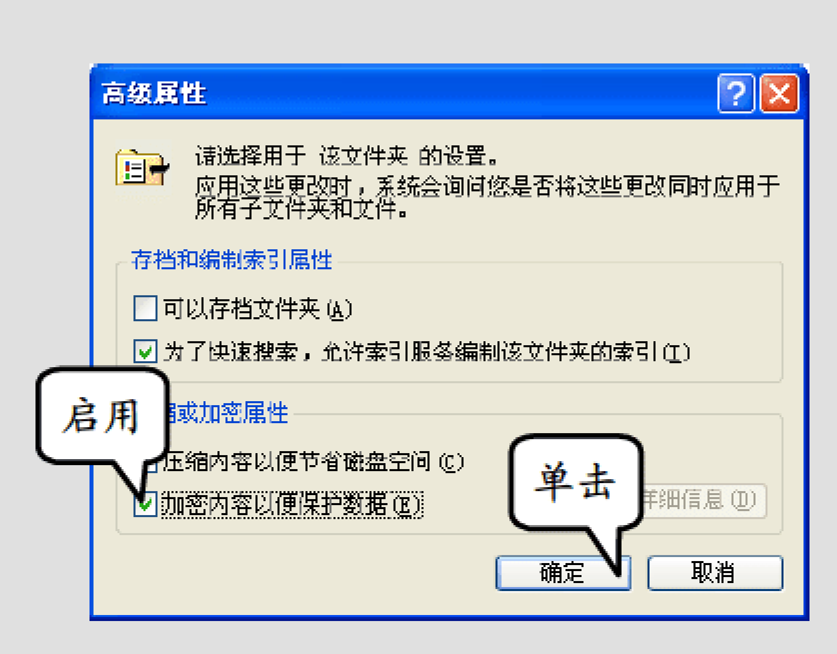


图 13-3　启用 EFS 加密

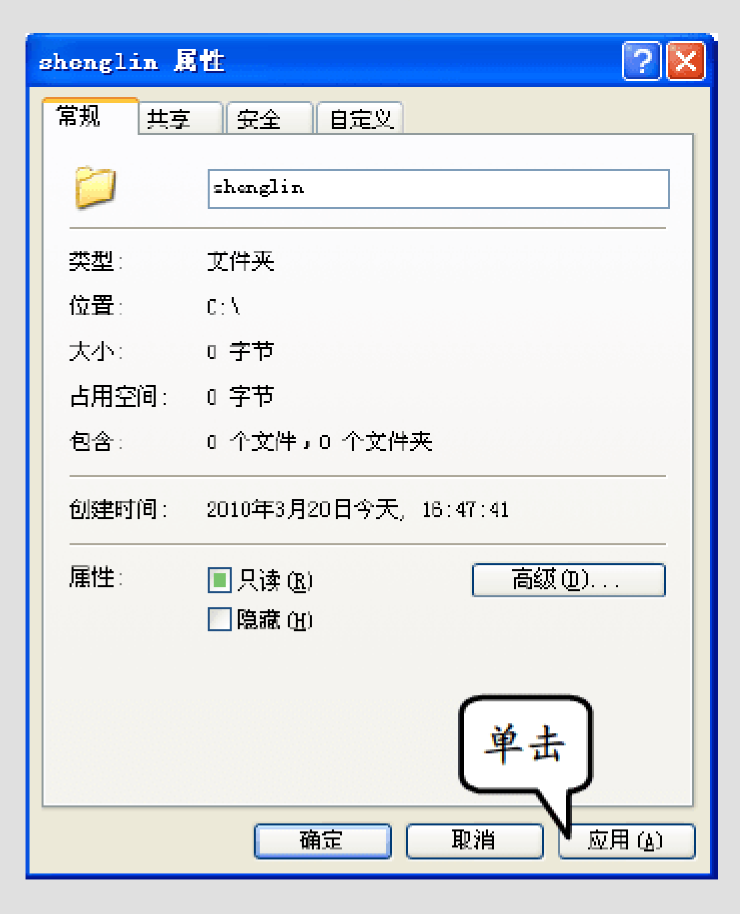


图 13-4　应用 EFS 加密

（5）在弹出的对话框中，选中【将更改应用于该文件夹、子文件和文件】单选按钮，单击【确定】按钮，如图 13-5 所示。

（6）在【本地磁盘（C:）】根目录中，可以查看到已加密的文件夹（文件名呈绿色），如图 13-6 所示。

（7）执行【开始】|【注销 administrator】命令，并在弹出的对话框中单击【注销】按钮，如图 13-7 所示。

（8）在 Windows 登录界面中，输入用户名和密码，并单击【确定】按钮，如图 13-8 所示。

（9）在【本地磁盘（C:）】根目录中，双击 shenglin 文件夹并双击【新建 文本文档】文

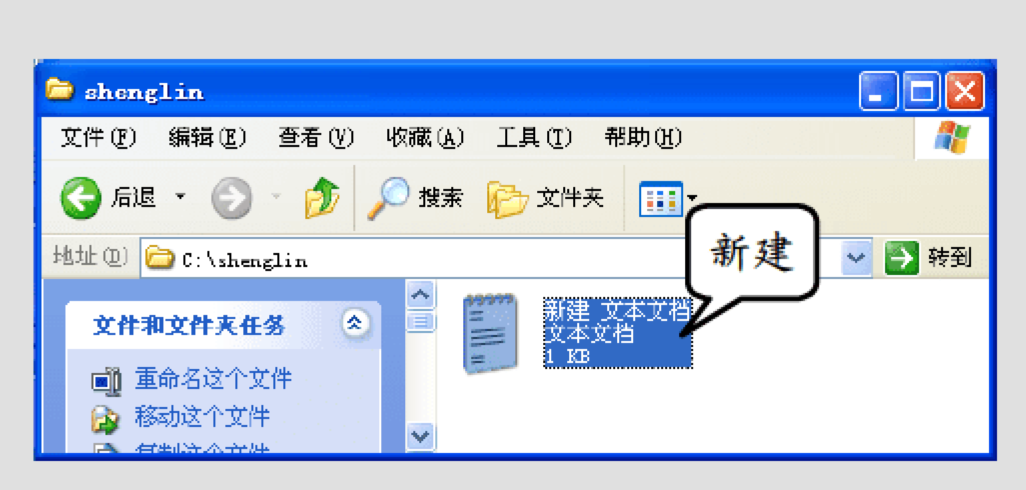


图 13-1　新建文本文档

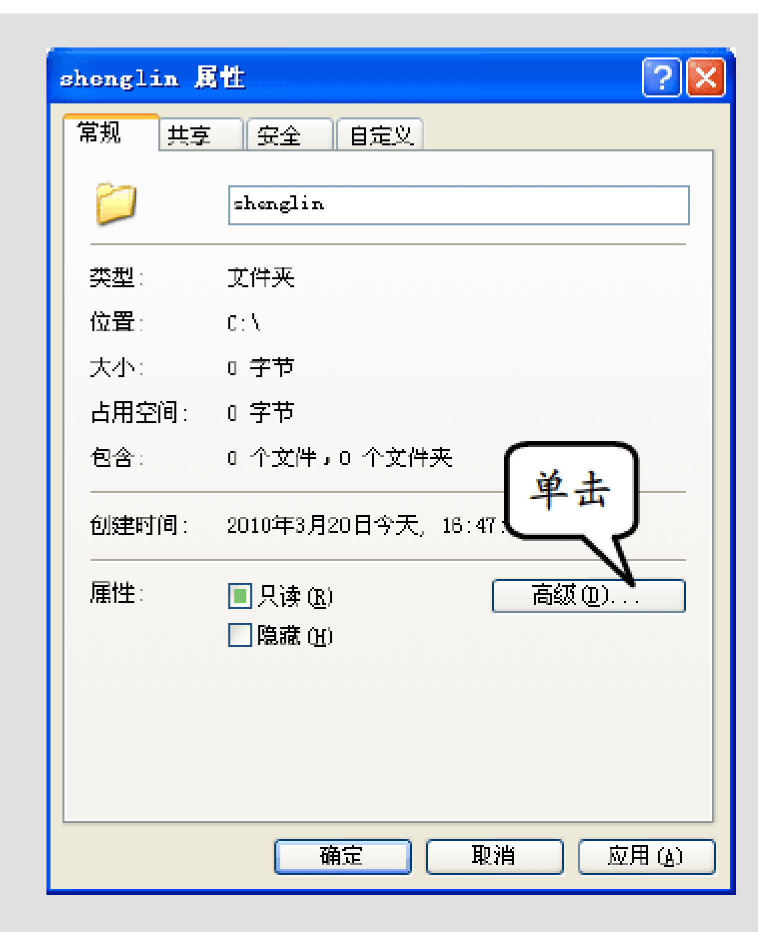


图 13-2　属性对话框

（3）在【高级属性】对话框中，启用【加密内容以便保护数据】复选框，单击【确定】按钮，如图 13-3 所示。



只有在 NTFS 分区才能进行 EFS 加密。

（4）在【shenglin 属性】对话框中，单击【应用】按钮，如图 13-4 所示。

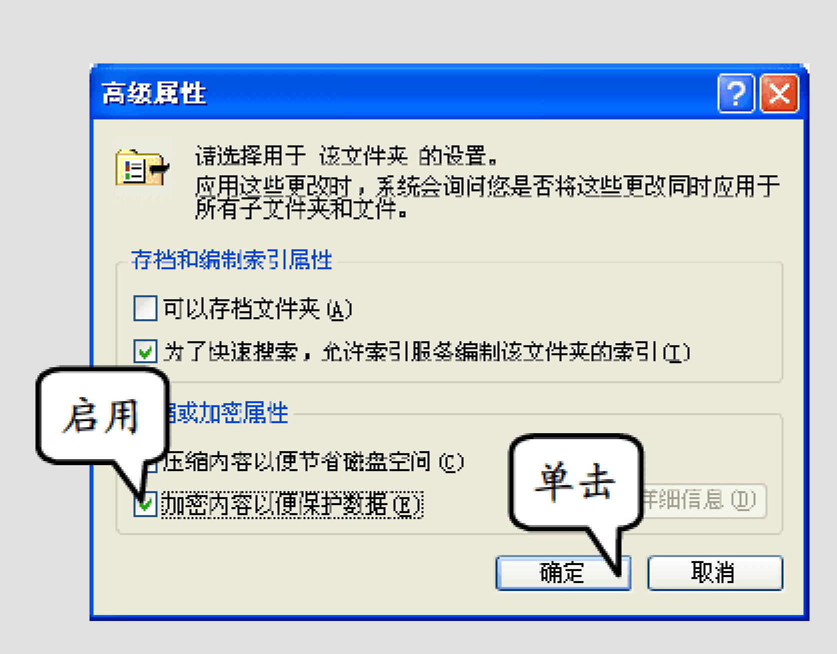


图 13-3　启用 EFS 加密

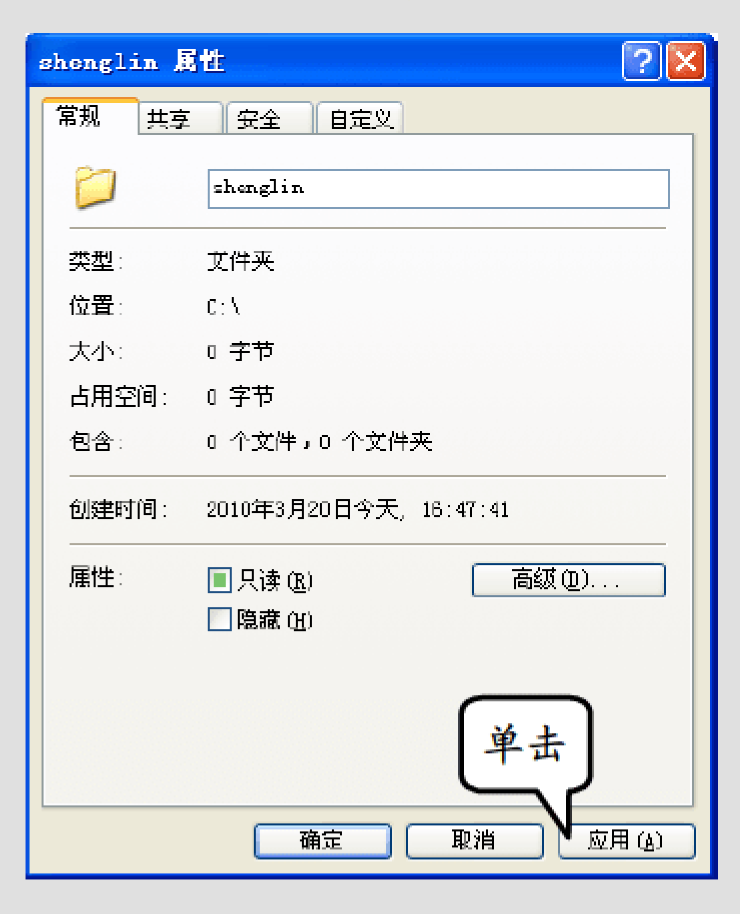


图 13-4　应用 EFS 加密

（5）在弹出的对话框中，选中【将更改应用于该文件夹、子文件和文件】单选按钮，单击【确定】按钮，如图 13-5 所示。

（6）在【本地磁盘（C:）】根目录中，可以查看到已加密的文件夹（文件名呈绿色），如图 13-6 所示。

（7）执行【开始】|【注销 administrator】命令，并在弹出的对话框中单击【注销】按钮，如图 13-7 所示。

（8）在 Windows 登录界面中，输入用户名和密码，并单击【确定】按钮，如图 13-8 所示。

（9）在【本地磁盘（C:）】根目录中，双击 shenglin 文件夹并双击【新建 文本文档】文

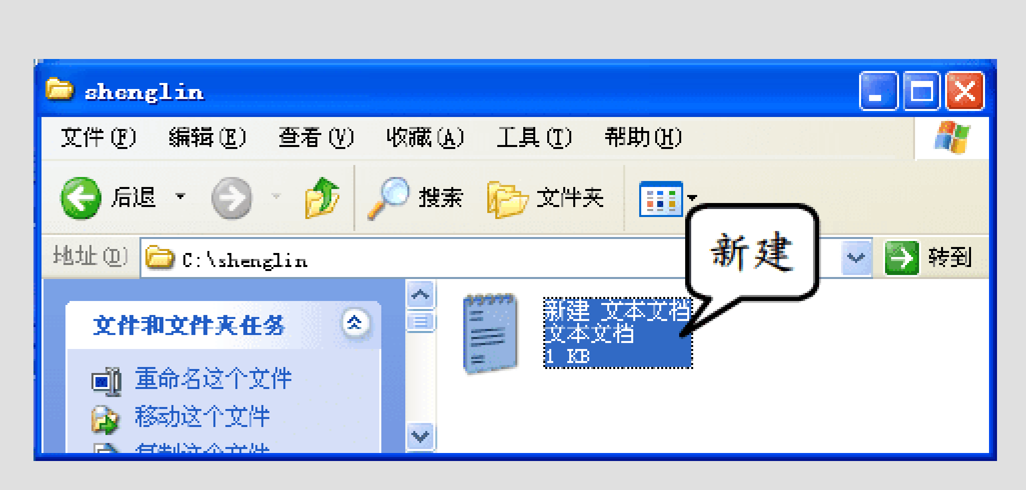


图 13-1　新建文本文档

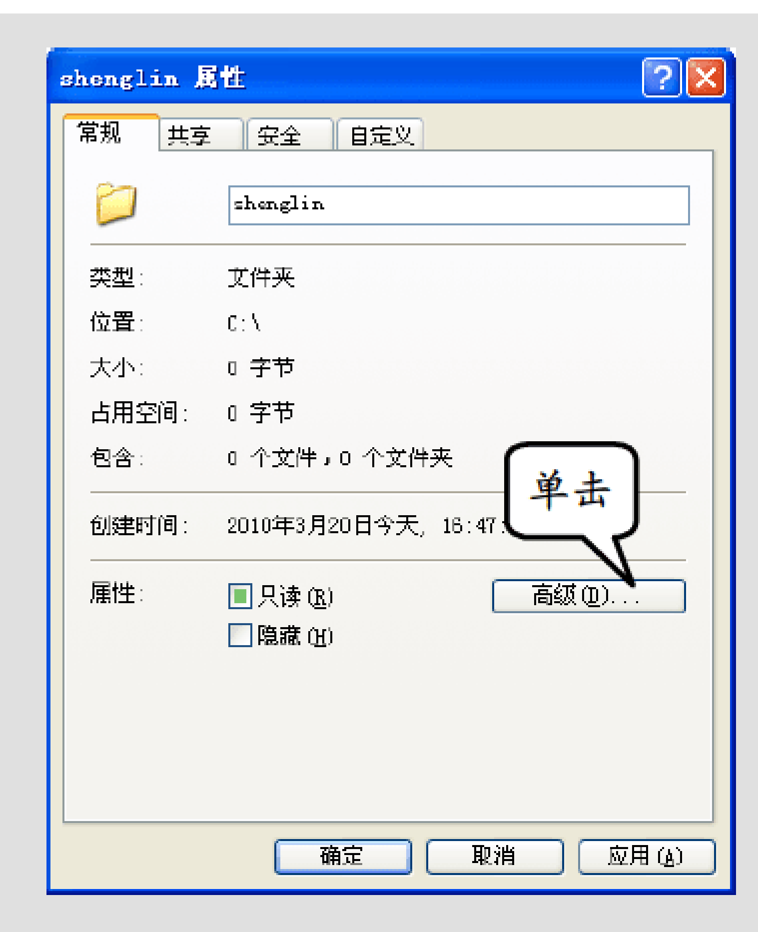


图 13-2　属性对话框

（3）在【高级属性】对话框中，启用【加密内容以便保护数据】复选框，单击【确定】按钮，如图 13-3 所示。



只有在 NTFS 分区才能进行 EFS 加密。

（4）在【shenglin 属性】对话框中，单击【应用】按钮，如图 13-4 所示。

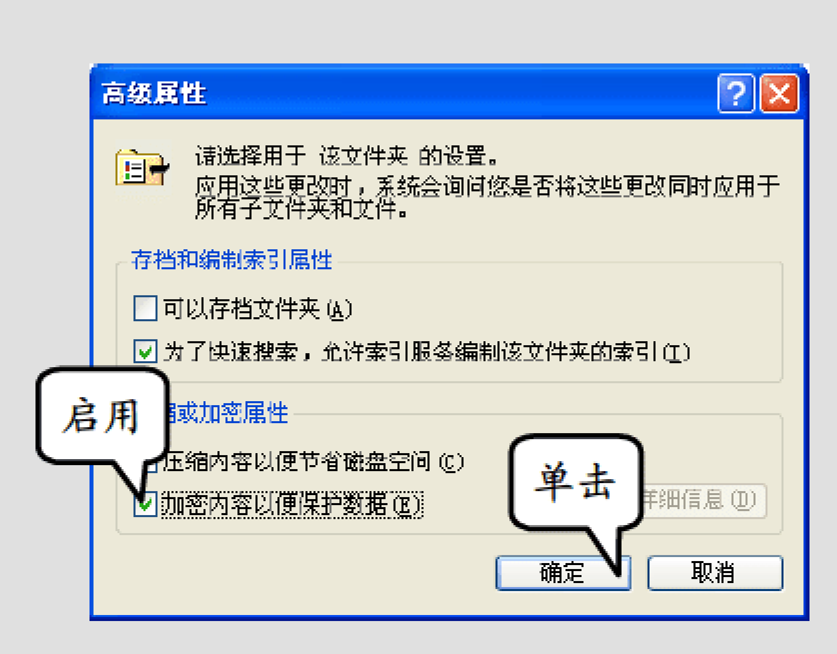


图 13-3　启用 EFS 加密

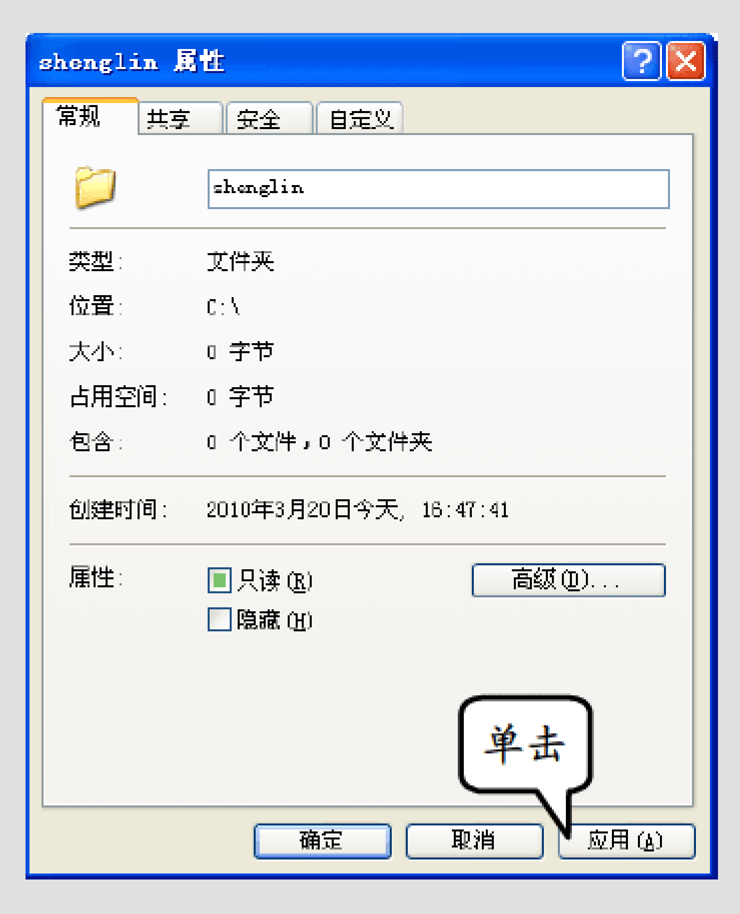


图 13-4　应用 EFS 加密

（5）在弹出的对话框中，选中【将更改应用于该文件夹、子文件和文件】单选按钮，单击【确定】按钮，如图 13-5 所示。

（6）在【本地磁盘（C:）】根目录中，可以查看到已加密的文件夹（文件名呈绿色），如图 13-6 所示。

（7）执行【开始】|【注销 administrator】命令，并在弹出的对话框中单击【注销】按钮，如图 13-7 所示。

（8）在 Windows 登录界面中，输入用户名和密码，并单击【确定】按钮，如图 13-8 所示。

（9）在【本地磁盘（C:）】根目录中，双击 shenglin 文件夹并双击【新建 文本文档】文

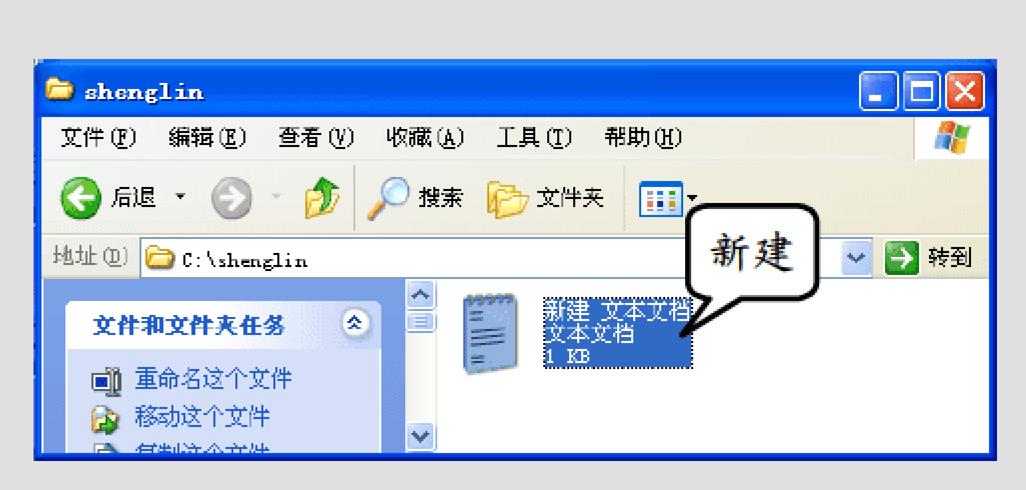


图 13-1　新建文本文档

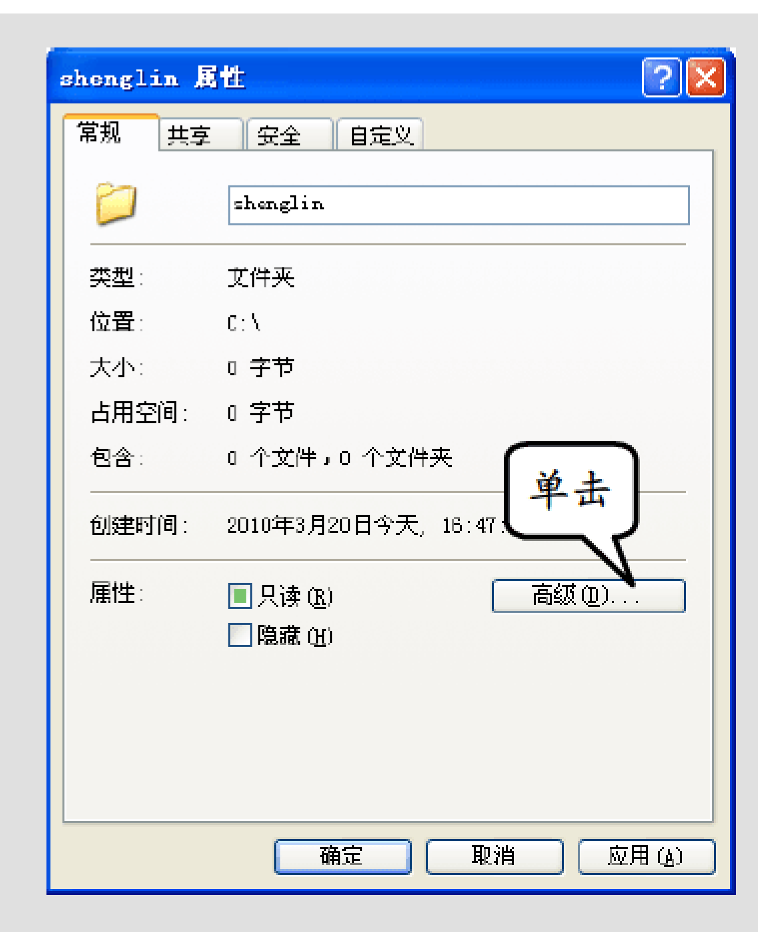


图 13-2　属性对话框

（3）在【高级属性】对话框中，启用【加密内容以便保护数据】复选框，单击【确定】按钮，如图 13-3 所示。



只有在 NTFS 分区才能进行 EFS 加密。

（4）在【shenglin 属性】对话框中，单击【应用】按钮，如图 13-4 所示。

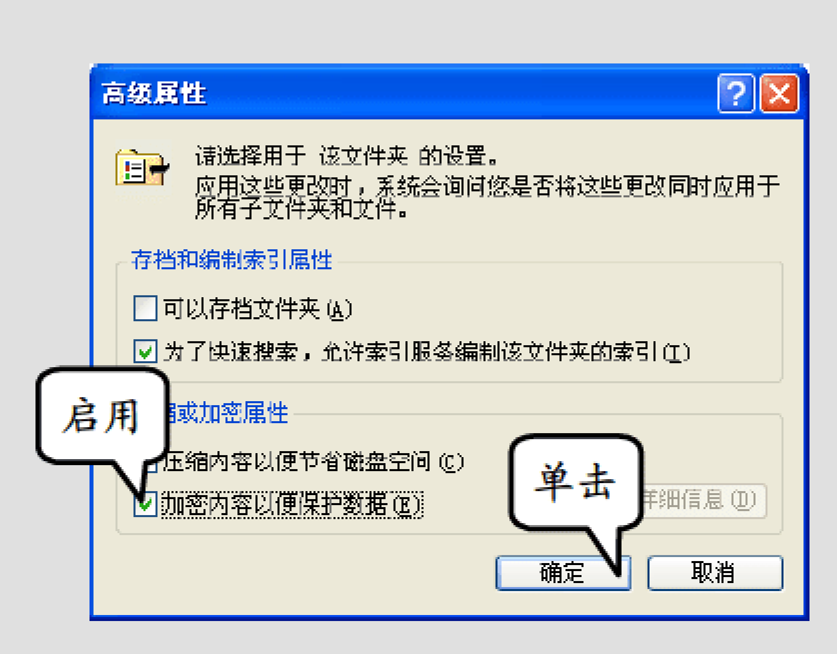


图 13-3　启用 EFS 加密

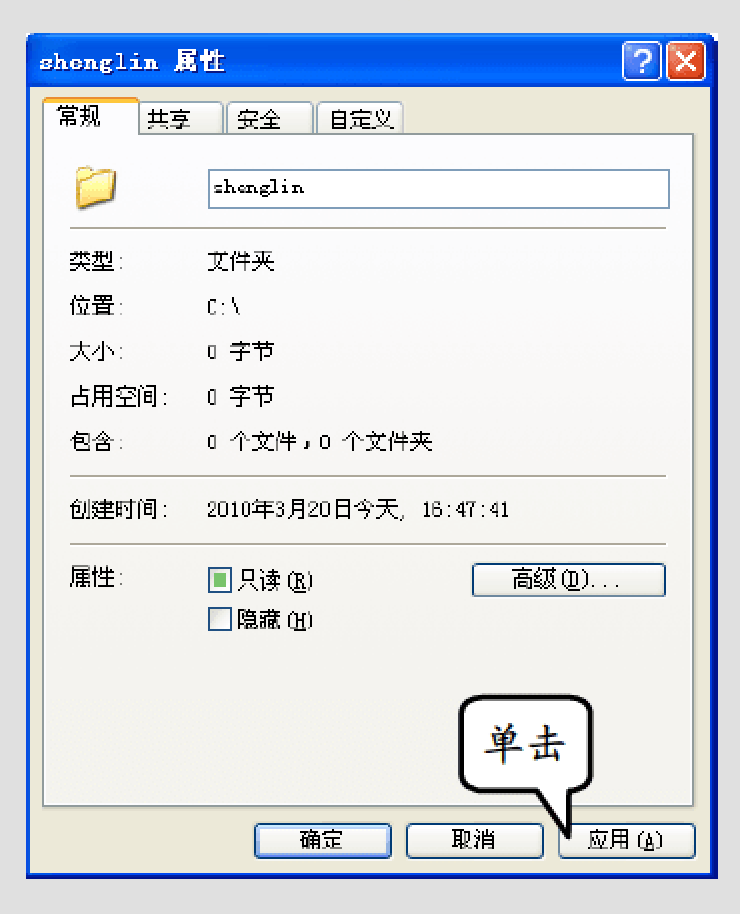


图 13-4　应用 EFS 加密

（5）在弹出的对话框中，选中【将更改应用于该文件夹、子文件和文件】单选按钮，单击【确定】按钮，如图 13-5 所示。

（6）在【本地磁盘（C:）】根目录中，可以查看到已加密的文件夹（文件名呈绿色），如图 13-6 所示。

（7）执行【开始】|【注销 administrator】命令，并在弹出的对话框中单击【注销】按钮，如图 13-7 所示。

（8）在 Windows 登录界面中，输入用户名和密码，并单击【确定】按钮，如图 13-8 所示。

（9）在【本地磁盘（C:）】根目录中，双击 shenglin 文件夹并双击【新建 文本文档】文

件，在弹出的对话框中，单击【关闭】按钮，如图 13-9 所示。

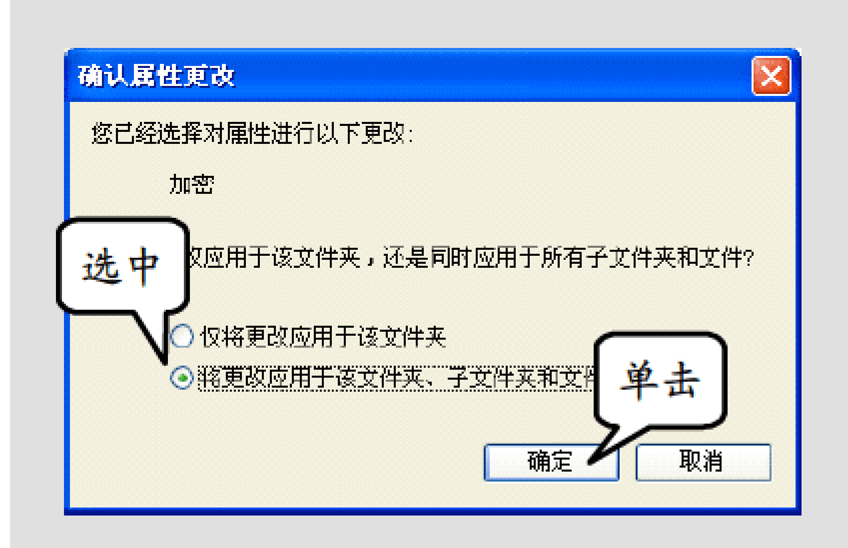


图 13-5　确定应用于文件夹和文件

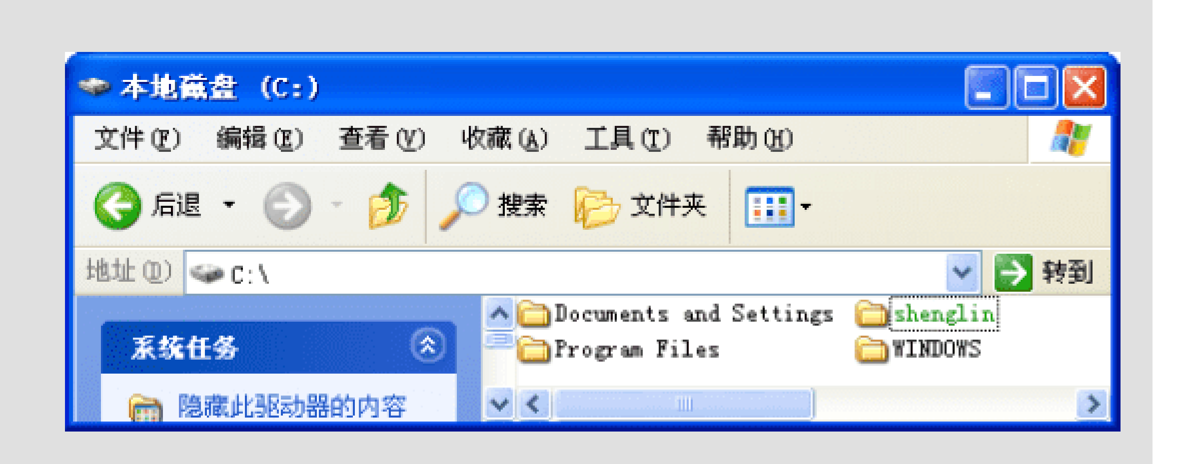


图 13-6　查看加密文件

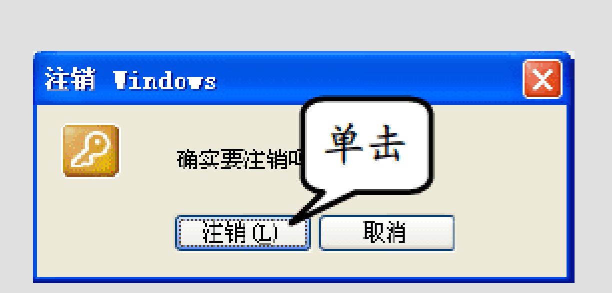


图 13-7　注销当前用户



图 13-8　使用 shenglin 登录



图 13-9　拒绝访问



使用 shenglin 这个用户登录后，拒绝访问被加密的文档，验证 EFS 加密的安全性。

13.3.2　操作实例——使用 EFS 加密后的共享

EFS 加密过的文件，只能由加密者或安装了加密证书的用户查看，这样造成网络共享不便的问题，而 EFS 加密后的共享，就解决了这个问题。

1. 实例目的

- ❑ 共享 EFS 加密后的文件。
- ❑ 查看 EFS 加密后的文件。

2. 实例步骤

（1）在桌面双击【我的电脑】图标，在弹出的窗口中双击【本地磁盘（C:）】图标，双击 shenglin 文件夹，右击执行【属性】命令，单击【高级】按钮，如图 13-10 所示。

（2）在【高级属性】对话框中，单击【详细信息】按钮，如图 13-11 所示。

（3）在弹出的对话框中，单击【添加】按钮，如图 13-12 所示。

（4）在【选择用户】对话框中，选择 shenglin 选项，单击【确定】按钮，如图 13-13 所示。

（5）在弹出的对话框中，依次单击【添加】和【确定】按钮，如图 13-14 所示。

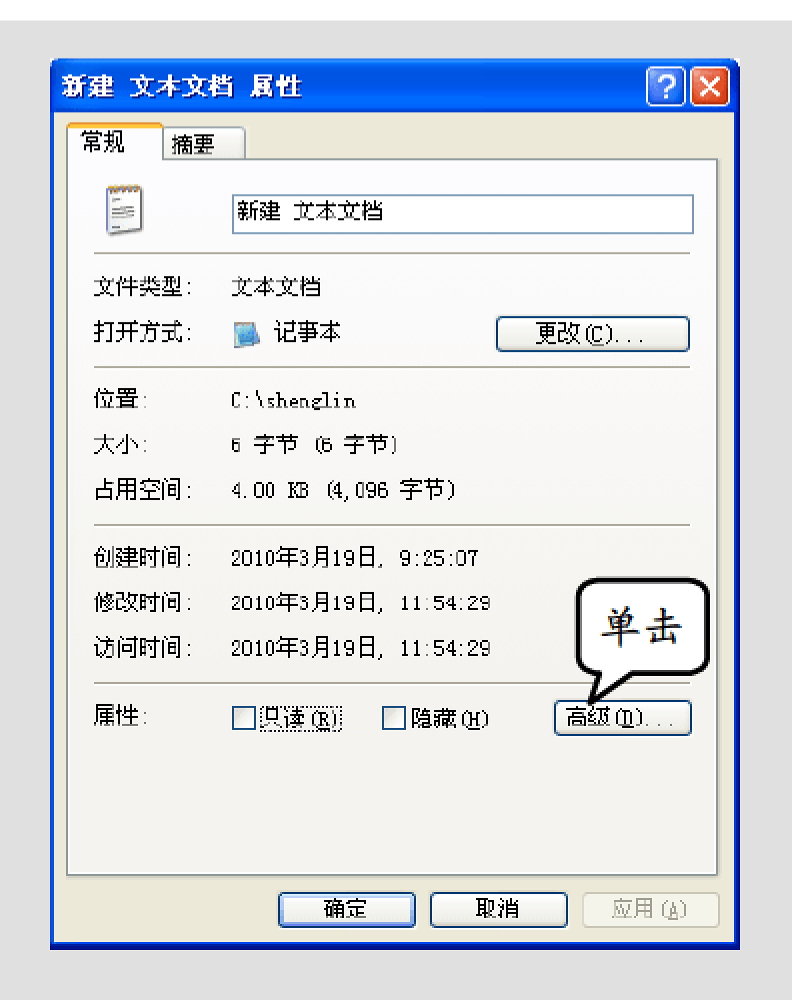


图 13-10　属性对话框

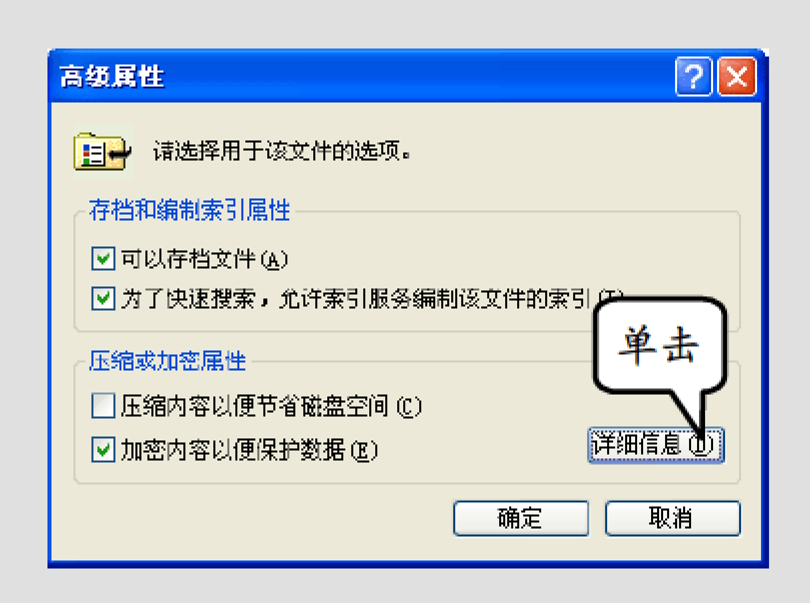


图 13-11　高级属性



图 13-12　单击【添加】按钮

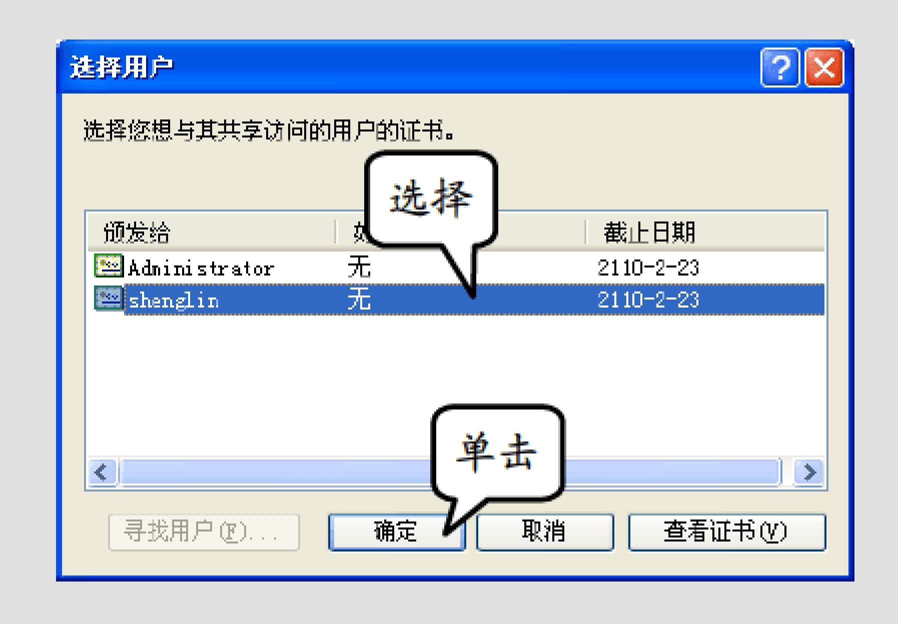
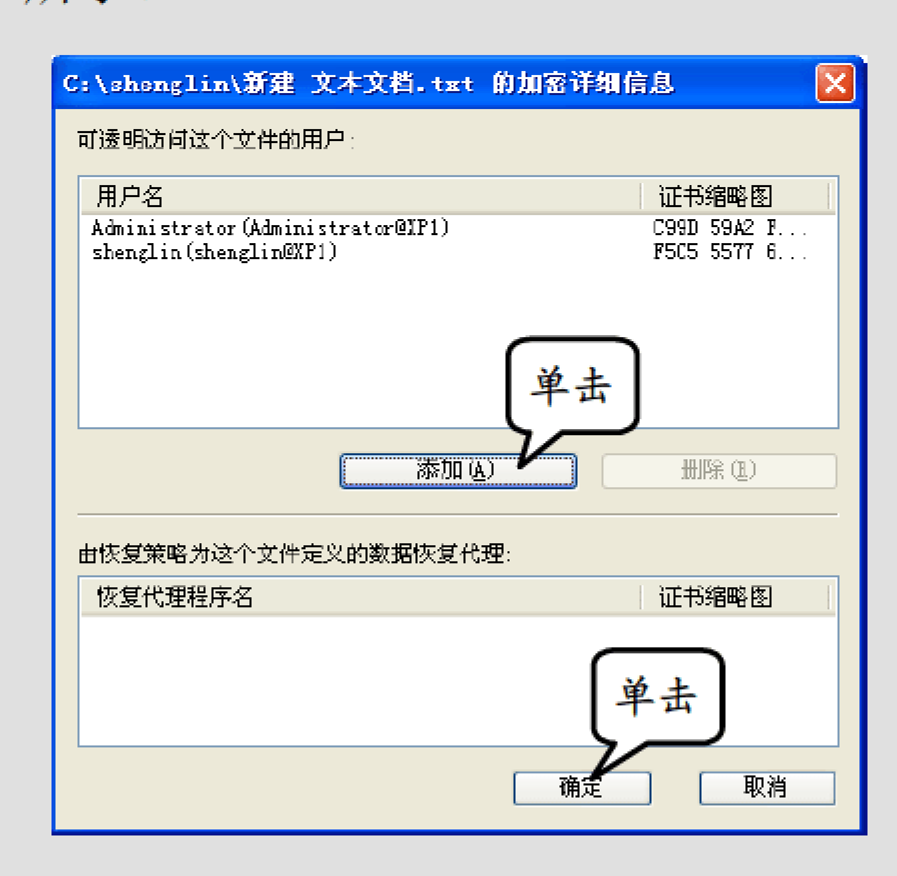


图 13-13　选择用户证书

（6）执行【开始】|【注销 administrator】命令，在弹出的对话框中单击【注销】按钮，如图 13-15 所示。



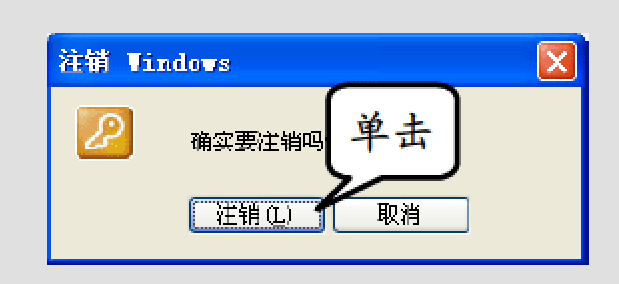


图 13-14　添加用户证书

图 13-15　注销当前用户

（7）在 Windows XP 登录界面中，输入用户名和密码，并单击【确定】按钮，如图 13-16 所示。

（8）在【本地磁盘（C:）】根目录中，双击 shenglin 文件夹，并在打开的窗口中，双击【新建 文本文档】文件，如图 13-17 所示。



图 13-16　使用 shenglin 登录

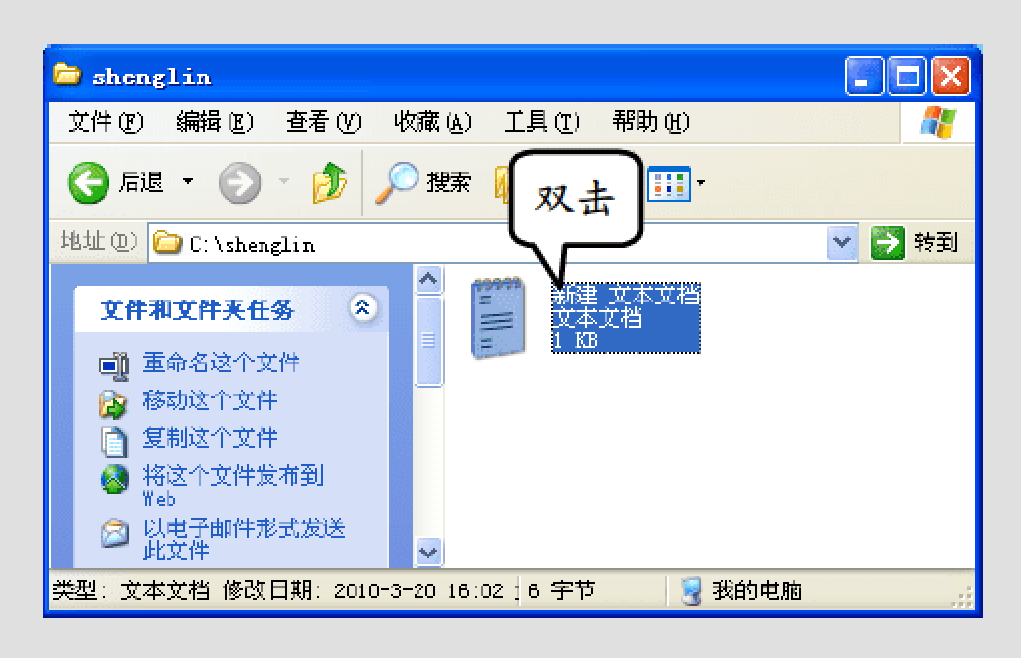


图 13-17　打开文档

（9）在【新建 文本文档—记事本】窗口中可查看到该文件内容，图 13-18 所示。

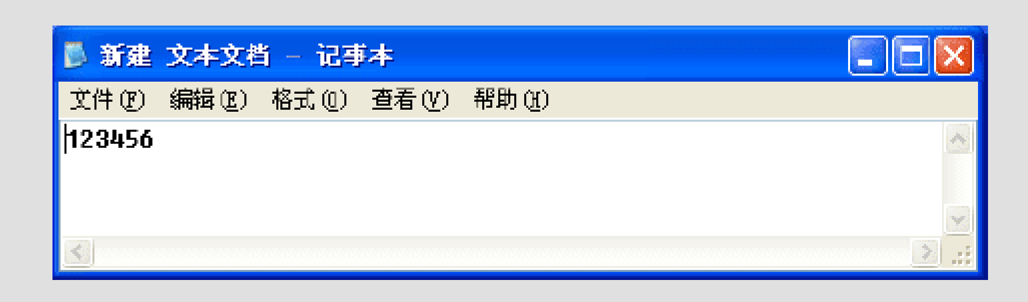


图 13-18　可以访问文档



使用 shenglin 这个用户，可以访问被加密的文档共享文档，验证 EFS 加密共享的实用性。

13.3.3　操作实例——密钥的备份和恢复

密钥的备份和恢复，有效地防止了密钥的损坏，解决了因重装系统或密钥丢失而导致的加密数据不能被解密的问题。

1. 实例目的

- 备份密钥。
- 恢复密钥。

2. 实例步骤

（1）在桌面执行【开始】|【运行】命令，在【运行】对话框中输入 certmgr.msc 命令，并单击【确定】按钮，如图 13-19 所示。

（2）在【证书】窗口中，依次展开【证书-当前用户】和【个人】节点，并选择【证书】选项，如图 13-20 所示。

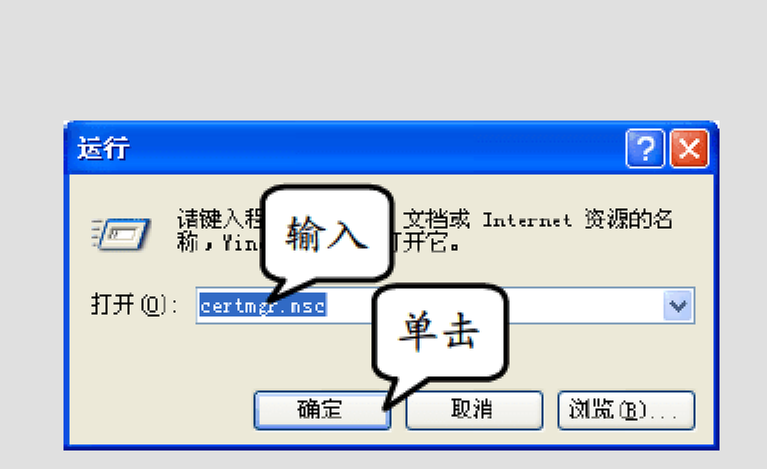


图 13-19　运行命令

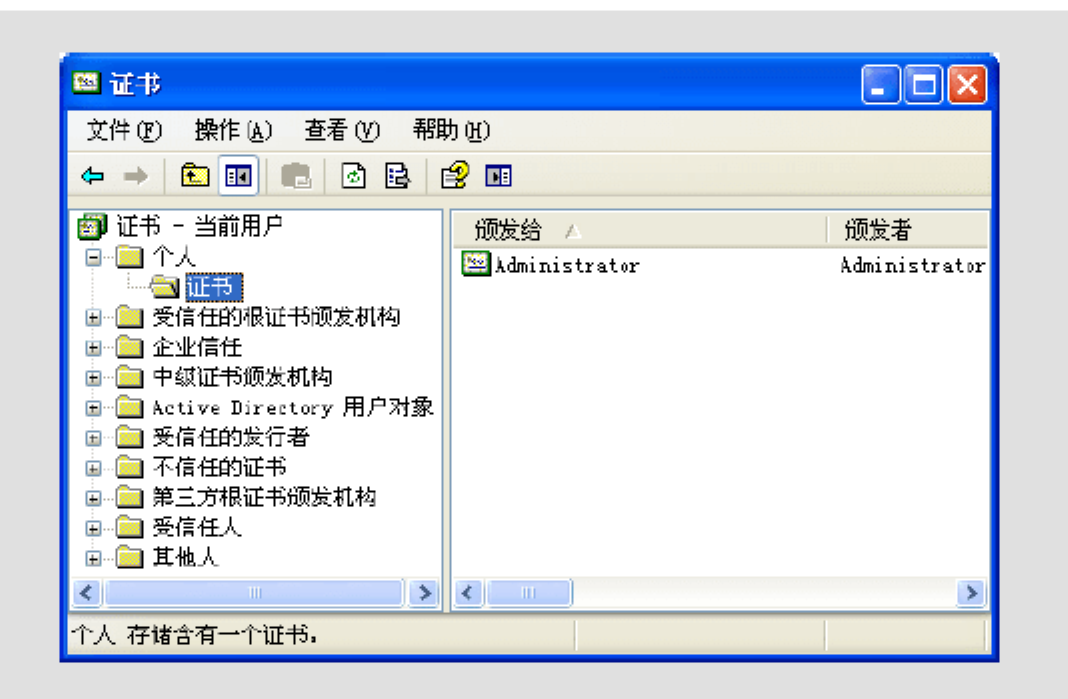


图 13-20　【证书】窗口

（3）右击 administrator 证书，执行【所有任务】|【导出】命令，如图 13-21 所示。

（4）在弹出的欢迎向导中，单击【下一步】按钮。在【导出私钥】对话框中，选中【是，导出私钥】单选按钮，并单击【下一步】按钮，如图 13-22 所示。

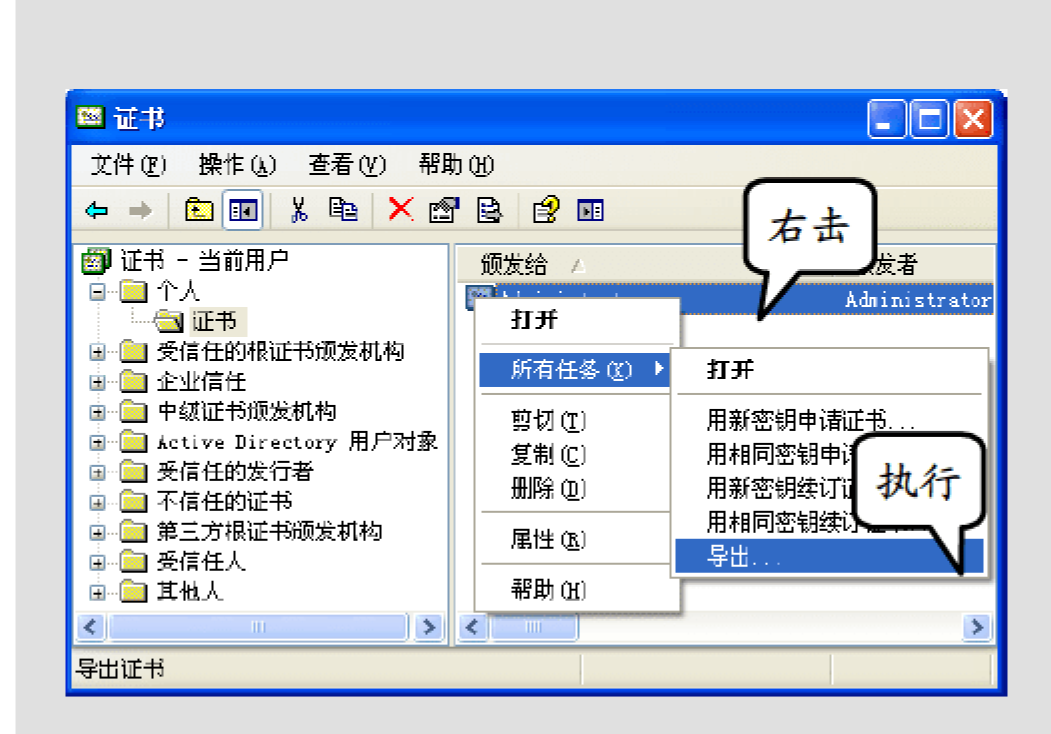


图 13-21　执行导出命令

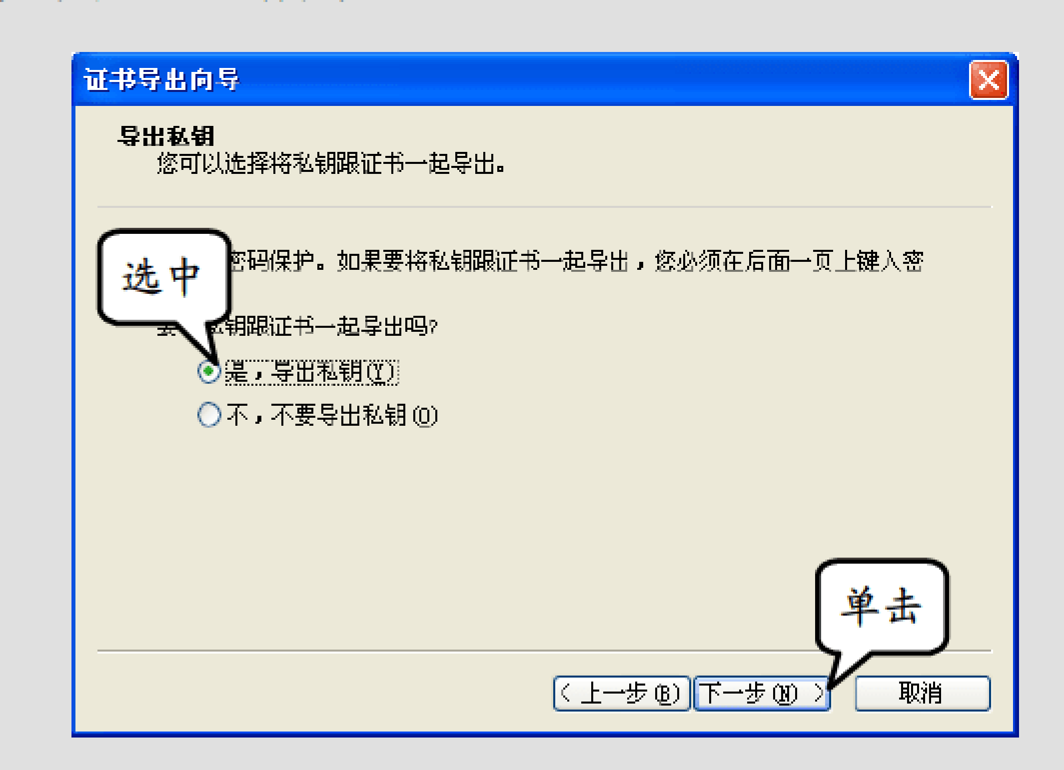


图 13-22　导出私钥

（5）在弹出的对话框中，单击【下一步】按钮，如图 13-23 所示。

（6）在【密码】对话框中的【密码】和【确认密码】文本框内输入相关内容，并单击【下一步】按钮，如图 13-24 所示。

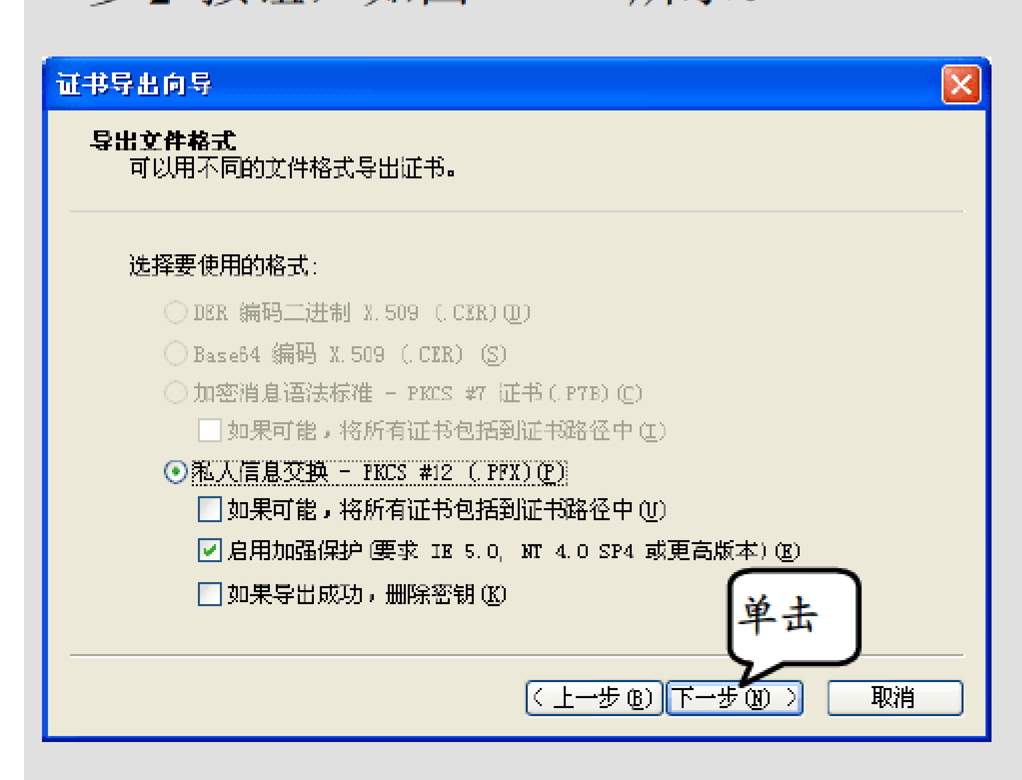


图 13-23　默认文件格式

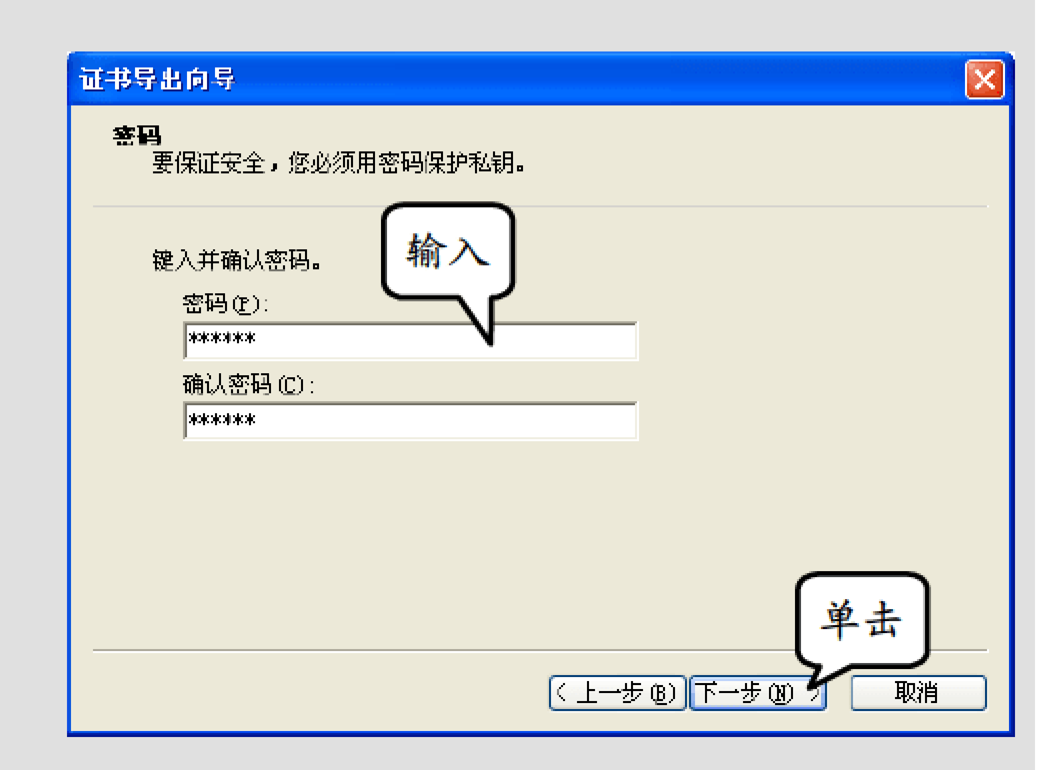


图 13-24　确认密码

（7）在弹出对话框的【文件名】文本框内输入“c：\Documents and Settings\Administrator\桌面\shenglin.pfx”文件路径（导出密钥的扩展名是 PFX），并单击【下一步】按钮，如图 13-25 所示。

（8）在【正在完成证书导出向导】对话框中，单击【完成】按钮，如图 13-26 所示。

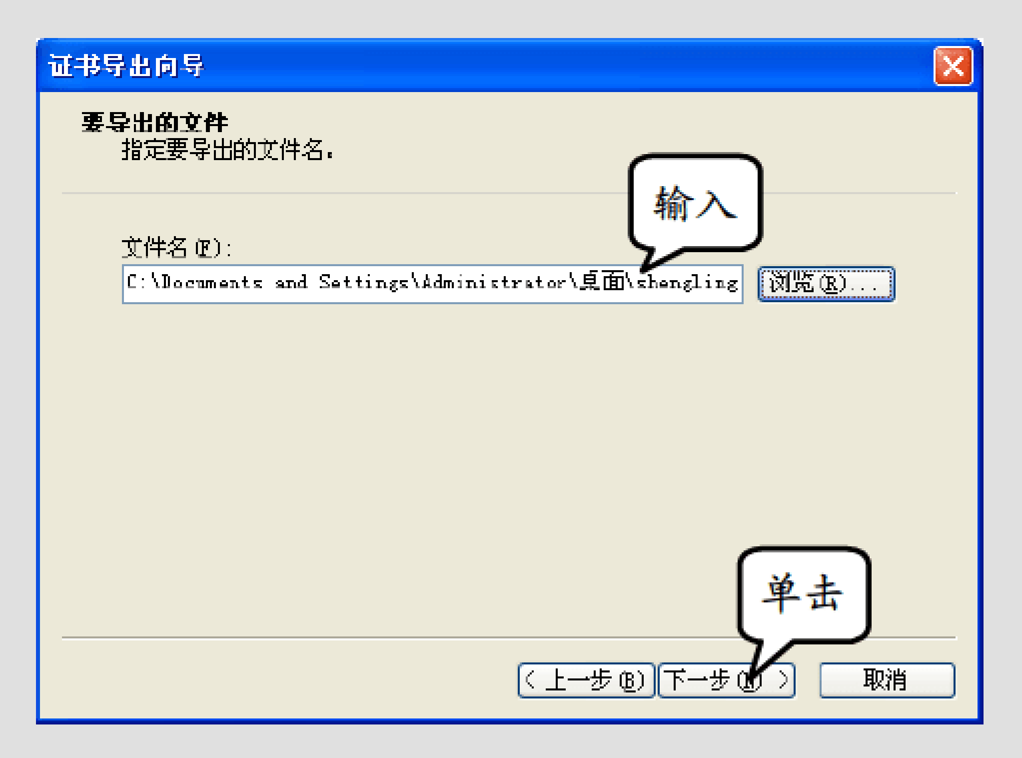


图 13-25　导出密钥的路径

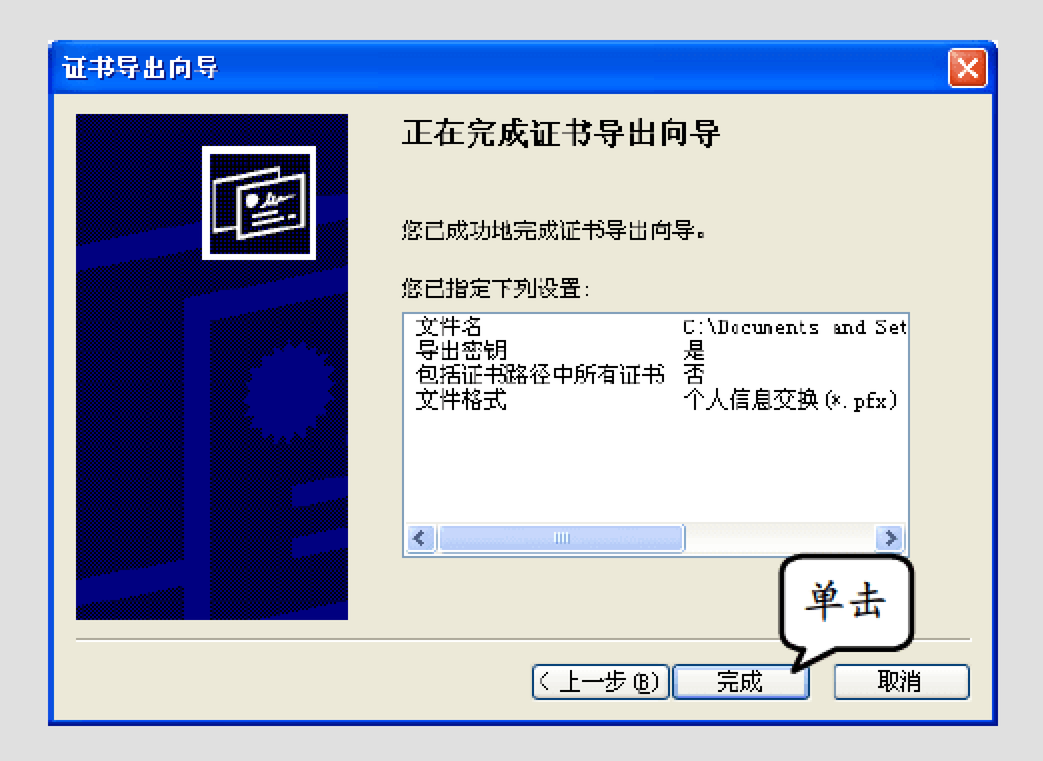


图 13-26　完成导出

（9）在弹出的对话框中，单击【确定】按钮，完成备份。

3. 恢复证书

（1）双击已备份的证书，在弹出的欢迎向导中，单击【下一步】按钮。在【要导入的文件】对话框中，单击【下一步】按钮，如图 13-27 所示。

（2）在【密码】对话框的【密码】文本框内输入相关内容，并单击【下一步】按钮，如图 13-28 所示。

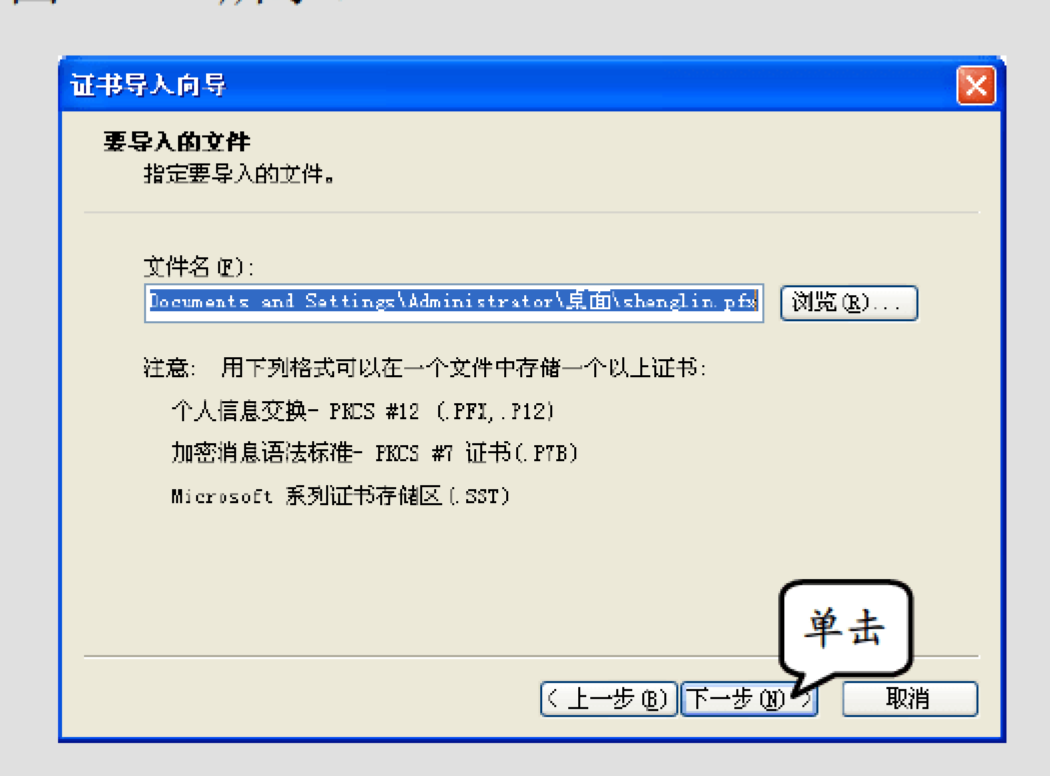


图 13-27　导入证书名称及信息

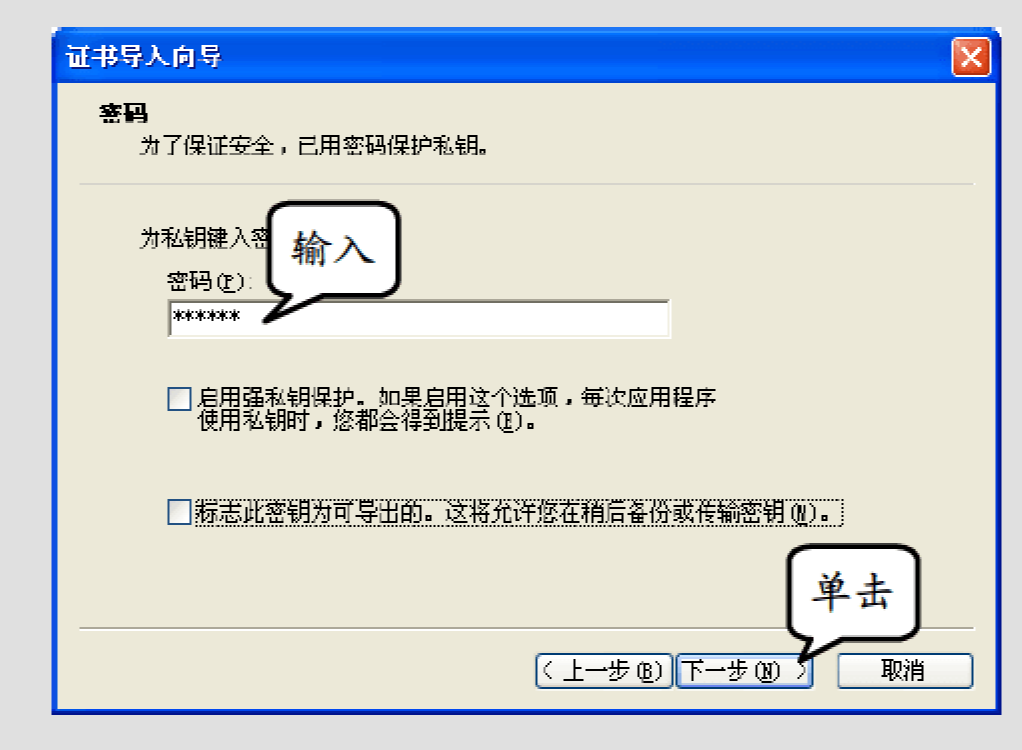


图 13-28　输入私钥密码

（3）在弹出的对话框中，单击【下一步】按钮，如图 13-29 所示。

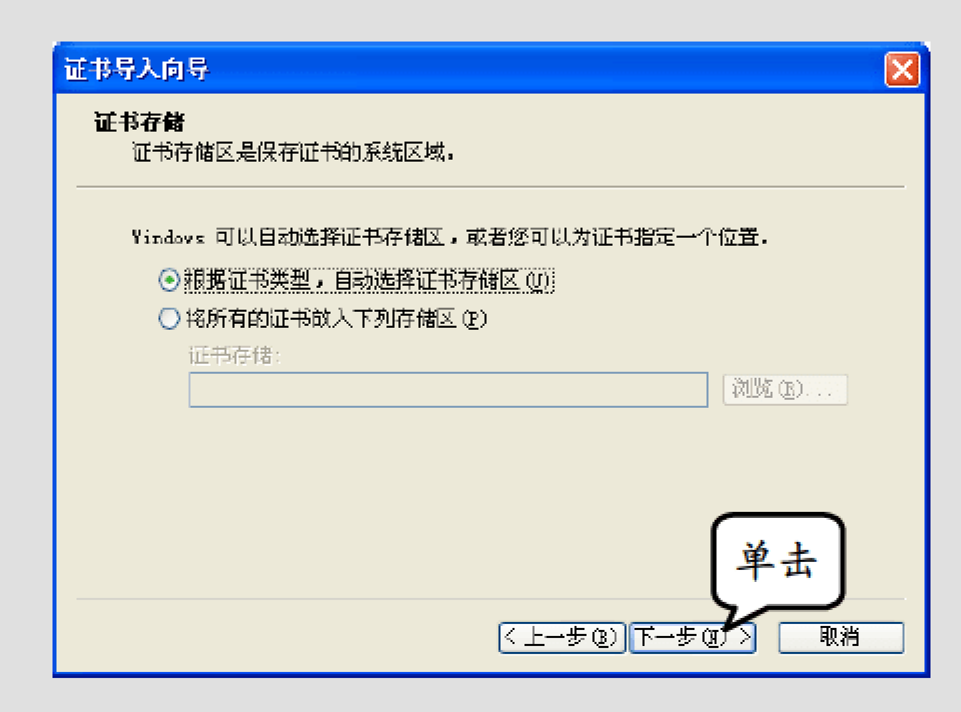


图 13-29　自动选择存储位置

（4）在【证书导入向导】对话框中，单击【完成】按钮，弹出“导入成功”提示。

13.4　数据及数据库备份

计算机里重要的数据、档案或历史记录，不论是对企业用户还是对个人用户，都是至关重要的，一旦不慎丢失，都会造成不可估量的损失，影响企业的正常运作，给科研、生产造成巨大的损失。因此，为了保障生产、销售、开发的正常运行，用户应当采取先进、有效的措施，对数据进行备份，防止意外的发生。

13.4.1　数据备份概述

数据备份是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用计算机的硬盘复制到其他存储介质的过程。传统的数据备份主要是采用内置或外置的磁带机进行冷备份。

但是这种方式只能防止操作失误等人为故障，而且其恢复时间也很长。随着技术的不断发展，数据的增加，有不少的企业开始采用网络备份。网络备份一般通过专业的数据存储管理软件结合相应的硬件和存储设备来实现。

1. 数据备份方式

通常，用户在对数据进行备份时，采用的方式有使用自带的数据备份程序、Ghost 数据备份及异地数据备份等。

❑ **Windows 系统自带数据备份程序**

WinZip（ZIP），WinRAR（RAR）压缩的备份或其他所有的数据备份软件，应该都会有选择所有的文件（不管文件是否有意动过都重新备份一次）和新增与变更的文件（只有新增或修改过的文件才会重新备份数据）两种选择。

❑ **Ghost 数据备份**

相信很多人都曾遇过计算机系统崩溃需要重新安装操作系统的事，其实若能在计算机刚安装好操作系统及应用程序后，且尚未建立数据文件前，先用 Ghost 软件将整个硬盘 ghost 成一个镜像文件，再刻录至 CD，日后在计算机需要重新安装时，只需用镜像文件即可还原当初硬盘的内容，可避免重新安装 Windows 和配置操作，既方便又省时。

❑ **异地数据备份**

将数据透过 Internet 网络或网络备份在另一个地（与计算机分离的存储介质，如软盘、Zip 磁盘、光盘以及存储卡等介质），好处是可避免因天灾导致同一个地区的计算机同时遭殃。目前，网络上也有提供 10MB 的免费空间给使用者放置个人数据，适用于数据量小的使用者。用网络备份要考虑到网速及安全性，不管采用何种备份方式，最好是将档案压缩成较小的容量后再传输，这样既省时间又省空间。

- **活备份**　备份到可擦写存储介质，以便更新和修改。
- **固定备份**　备份到不可擦写的存储介质（如只读存储器 CD-ROM），以防错误删

除和别人有意篡改。这还是备份的硬件级问题。

➢ **动态备份** 利用软件功能定时自动备份指定文件，或文件内容产生变化后随时自动备份。

➢ **静态备份** 为保持文件原貌而进行人工备份。

2. 备份资料

备份资料即对重要数据如文档、数据库、记录、进度等备份下来生成一个备份文件放在安全的存储空间内，当发生数据被破坏或丢失时可将原备份文件恢复到备份时状态。

❑ Office 文档（.doc .xls .ppt 等格式的文件）。
❑ 客户数据、会计数据等数据库 Database 文件。
❑ 邮件文档，如 Outlook 之 .pst、.dbx 及通讯录 .wab。
❑ 重要图档，如.pdf、.bmp、.tiff、.dwg 和.jpg。
❑ Linux 系统本机上数据的手工备份。

例如，Linux 系统上配有功能强大的 tar 命令，可以灵活地备份数据。tar 最初是为了制作磁带备份而设计的，把文件和目录备份到磁带中，然后从磁带中提取或恢复文件。当然，现在可以使用 tar 来备份数据到任何存储介质上。tar 非常易于使用，稳定可靠，而且在任何 Linux 系统上都有这个命令。因此是最经常使用的备份工具。使用 tar 命令备份数据的语法格式如下所示。

```
$ tar cvf backup.tar /home/html
```

上述命令是将/home/html 目录下的所有文件打包成 tar 文件 backup.tar。cvf 是 tar 的命令参数。

❑ c 代表创建一个档案文件。
❑ v 代表显示每个备份的文件名字。
❑ f 表示 tar 创建的档案文件名是后面的 backup.tar。
❑ /home/html 代表 tar 要备份的文件或和目录名。

使用 tar 命令恢复数据的语法格式如下所示。

```
$ tar xvf backup.tar
```

上述命令将备份文件 backup.tar 恢复到当前目录下。通常，tar 对文件进行备份的时候并不对文件进行压缩，因此备份文件的尺寸非常大。

另外，使用$ tar zcvf backup.tar /home/html 命令，能够使 tar 在备份结束以后，自动使用 gzip 命令对备份文件进行压缩，得到一个相应的 gz 文件。这样，可以得到两个文件，backup.tar 和 backup.tar.gz。backup.tar.gz 是压缩的备份文件。

3. 数据备份日常维护

备份系统安装调试成功结束后，日常维护包含两方面工作，即硬件维护和软件维护。如果硬件设备具有很好的可靠性，系统正常运行后基本不需要经常维护。

一般来说，磁带库的易损部件是磁带驱动器，当出现备份读写错误时应首先检查驱动器

的工作状态。如果发生意外断电等情况，系统重新启动运行后，应检查设备与软件的连接是否正常。磁头自动清洗操作一般可以由备份软件自动管理，一盘 DLT（Digital Linear Tape，数字线性磁带）清洗带可以使用 20 次，一般一个月清洗一次磁头。软件系统工作过程检测到的软硬件错误和警告信息都有明显提示和日志，可以通过电子邮件发送给管理员。管理员也可以利用远程管理的功能，全面监控备份系统的运行情况。

网络数据备份系统的建成，对保障系统的安全运行，保障各种系统故障的及时排除和数据库系统的及时恢复起到关键作用。通过自动化磁带库及集中的运行管理，保证数据备份的质量，加强数据备份的安全管理。同时，近线磁带库技术的引进，无疑对数据的恢复和利用提供了更加方便的手段。

13.4.2 数据库备份及恢复

保障网络系统的顺利运行，是每个用户最为关心的问题。而网络备份的最终目的，就是要解决这个问题。所以，一份优秀的网络备份方案就要能够备份系统所有的数据，在网络出现故障甚至损坏时，能够迅速地恢复网络系统和数据。从发现故障到完全恢复系统，理想的备份方案耗时不应超过半个工作日。这样，如果系统出现灾难性故障，就可以把损失降到最低。

在选择备份系统时，既要做到满足系统容量不断增加的需求，又需要所用的备份软件能够支持多平台系统。要做到这些，就要充分使用网络数据存储管理系统，它是在分布式网络环境下，通过专业的数据存储管理软件，结合相应的硬件和存储设备，对网络的数据备份进行集中管理，从而实现自动化的备份、文件归档、数据分级存储及灾难恢复等。

通常，一个完整的数据备份和灾难恢复方案，应包括备份模式的设定、备份硬件、备份软件、备份计划和灾难恢复计划 5 个部分。

1. 备份模式的设定

备份模式一般分为 LAN（局域网）备份、LAN Free（局域网连接的存储）备份和 SAN Server-Free（存储区域网）备份三种。LAN 备份针对所有存储类型都可以使用，LAN Free 备份和 SAN Server-Free 备份只能针对 SAN 架构的存储。

- **基于 LAN 备份**

传统备份需要在每台计算机上安装磁带机备份本机系统，采用 LAN 备份策略，在数据量不是很大的时候，可采用集中备份。一台中央备份服务器将会安装在 LAN 中，然后将应用服务器和工作站配置为备份服务器的客户端。中央备份服务器接受运行在客户机上的备份代理程序的请求，将数据通过 LAN 传递到它所管理的、与其连接的本地磁带机资源上。这一方式提供了一种集中的、易于管理的备份方案，并通过在网络中共享磁带机资源提高了效率。

- **基于 LAN Free 和 SAN Server-Free 备份**

由于数据通过 LAN 传播，当需要备份的数据量较大，备份时间窗口紧张时，网络容易发生堵塞。因此在 SAN（网络存储）环境下，可采用存储网络的 LAN-Free 备份，需要备份的服务器通过 SAN 连接到磁带机上，在 LAN-Free 备份客户端软件的触发下，读取需要备份的数据，通过 SAN 备份到共享的磁带机。这种独立网络不仅可以使 LAN 流量得以转移，而且

它的运转所需的CPU资源低于LAN方式，这是因为光纤通道连接不需要经过服务器的TCP/IP栈，而且某些层的错误检查可以由光纤通道内部的硬件完成。

在许多解决方案中需要一台计算机来管理共享的存储设备，以及用于查找和恢复数据的备份数据库。LAN Free 备份需要占用备份计算机的 CPU 资源，如果备份过程能够在 SAN 内部完成，而大量数据流无需流过服务器，则可以极大地降低备份操作对生产系统的影响，SAN Server-Free 备份就是这样的技术。

如何选择用户的备份模式，要根据用户的实际情况而定。

2. 备份硬件

一般说来，丢失数据有人为的错误、漏洞和病毒、设备故障 3 种可能。针对这些问题，目前较流行的解决方法包括硬盘介质存储、光学介质和磁带或磁带机存储技术。

与磁带或磁带机存储技术和光学介质备份相比，硬盘存储所需费用是极其昂贵的。磁盘存储技术虽然可以提供容错性解决方案，但容错却不能抵御用户的错误和病毒。一旦两个磁盘在短时间内失灵，在一个磁盘重建之前，不论是磁盘镜像还是磁盘双工都不能提供数据保护。因此，在大容量数据备份方面，采用硬盘作为备份介质并不是最佳选择。

与硬盘备份相比，虽然光学介质备份提供了比较经济的存储解决方案，但它们所用的访问时间要比硬盘长 2～6 倍，并且容量相对较小。当备份大容量数据时，所需光盘数量大；虽保存的持久性较长，但整体可靠性较低。所以光学介质也不是大容量数据备份的最佳选择。

在大容量备份方面，磁带机所具有的优势是容量大并可灵活配置、速度相对适中、介质保存长久，存储时间超过 30 年、成本较低、数据安全性高、可实现无人操作的自动备份等。所以一般来说，磁带设备是大容量网络备份用户的主要选择。

3. 备份软件

虽然已有用户在网络中运用到大容量备份设备，但大多数用户还没有意识到备份软件的重要性。重要原因是许多人对备份知识和备份手段缺乏了解。他们所知道的备份软件无非是网络操作系统附带提供的备份功能，但对如何正确使用专业的备份软件却知之甚少。

通常，备份软件主要分两大类，一是各个操作系统厂商在软件内附带的，如 NetWare 操作系统的“Backup”功能、NT 操作系统的“NTBackup”等；二是专业备份软件厂商提供的全面的专业备份软件，如 CA 公司的 BrightStor ARCserve Backup V9。

对于备份软件的选择，不仅要注重使用方便、自动化程度高，还要有好的扩展性和灵活性。同时，跨平台的网络数据备份软件能满足用户在数据保护、系统恢复和病毒防护方面的支持。一个专业的备份软件配合高性能的备份设备，能够使损坏的系统迅速得到恢复。

4. 备份策略

灾难恢复的先决条件，是要做好备份策略及恢复计划。日常备份计划描述每天的备份以什么方式进行、使用什么介质、什么时间进行以及系统备份方案的具体实施细则。在计划制定完毕后，应严格按照程序进行日常备份，否则将无法达到备份的目的。目前被采用最多的备份策略主要有以下 3 种。

❑ 完全备份（full backup）

每天对自己的系统进行完全备份。例如，星期一用一盘磁带对整个系统进行备份，星期二再用另一盘磁带对整个系统进行备份，以此类推。这种备份策略的好处是：当发生数据丢失的灾难时，只要用一盘磁带（即灾难发生前一天的备份磁带），就可以恢复丢失的数据。

然而它也有不足之处，首先，由于每天都对整个系统进行完全备份，造成备份的数据大量重复。这些重复的数据占用了大量的磁带空间，这对用户来说就意味着增加成本。其次，由于需要备份的数据量较大，因此备份所需的时间也就较长。对于那些业务繁忙、备份时间有限的单位来说，选择这种备份策略是不明智的。

❑ 增量备份（incremental backup）

星期天进行一次完全备份，然后在接下来的六天里只对当天新的或被修改过的数据进行备份。这种备份策略的优点是节省了磁带空间，缩短了备份时间。但它的缺点是当灾难发生时，数据的恢复比较麻烦。

例如，系统在星期三的早晨发生故障，丢失了大量的数据，那么现在就要将系统恢复到星期二晚上时的状态。这时系统管理员就要首先找出星期天的那盘完全备份磁带进行系统恢复，然后再找出星期一的磁带来恢复星期一的数据，然后找出星期二的磁带来恢复星期二的数据。很明显，这种方式很烦琐。另外，这种备份的可靠性也很差。在这种备份方式下，各盘磁带间的关系就像链子一样，一环套一环，其中任何一盘磁带出了问题都会导致整条链子脱节。比如在上例中，若星期二的磁带出了故障，那么管理员最多只能将系统恢复到星期一晚上时的状态。

❑ 差异备份（differential backup）

管理员先在星期天进行一次系统完全备份，然后在接下来的几天里，管理员再将当天所有与星期天不同的数据（新的或修改过的）备份到磁带上。

差异备份策略在避免了以上两种策略的缺陷的同时，又具有了它们的所有优点。首先，它无需每天都对系统做完全备份，因此备份所需时间短，并节省了磁带空间，其次，它的灾难恢复也很方便。系统管理员只需两盘磁带，即星期一磁带与灾难发生前一天的磁带，就可以将系统恢复。

在实际应用中，备份策略通常是以上 3 种的结合。例如，每周一至周六进行一次增量备份或差异备份，每周日进行全备份，每月底进行一次全备份，每年底进行一次全备份。

5. 灾难恢复

灾难恢复措施在整个备份中占有相当重要的地位。因为它关系到系统、软件与数据在经历灾难后能否快速、准确地恢复。全盘恢复一般应用在服务器发生意外灾难，导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等情况，也称为系统恢复。此外，有些厂商如惠普还推出了拥有单键恢复（OBDR）功能的磁带机，只需用系统盘引导机器启动，将磁带插入磁带机，按动一个按键即可恢复整个系统。

13.5 数据恢复工具

重要数据一旦破坏，用户将承受巨大的损失，所以数据恢复产业应运而生。数据恢复工

具用来在数据丢失和损坏时挽救这些数据，可以基于各种软、硬件平台开展。针对文件的误删除，存储设备受到严重破坏等情况，专业的数据恢复工作都可能将数据恢复。

13.5.1 FinalData

在 Windows 环境下删除一个文件，只是将目录信息从 FAT 或者 MFT（NTFS）删除，这意味着文件数据仍然留在磁盘上。所以，从技术角度来讲，这个文件是可以恢复的。FinalData 就是通过这个机制来恢复丢失的数据的，在清空回收站以后也不例外。

另外，FinalData 可以很容易地从格式化后的文件和被病毒破坏的文件恢复。甚至在极端的情况下，如果目录结构被部分破坏也可以恢复，只要数据仍然保存在硬盘上。为了确保在 Windows XP、Windows Server 2003 或 Windows Server 2008 上的高恢复率，在系统中必须事先安装文件保护和删除检测，这可以通过安装 FinalData 2.0 来实现。

启动 FinalData2.0 安装程序，可通过双击下载的安装程序 setup.exe，然后在【欢迎】对话框中单击【下一步】按钮，当出现【软件许可证协议】对话框时，单击【是】按钮，如图 13-30 所示。

接受软件的许可协议后，在【请输入用户注册信息】对话框中，输入注册用户姓名、公司名称及该软件的序列号，然后单击【下一步】按钮，如图 13-31 所示。其中，注册用户名称和公司名称可随意填写，但产品序列号必须输入正确（此序列号发布在该软件的下载网站上），否则安装将不能继续。

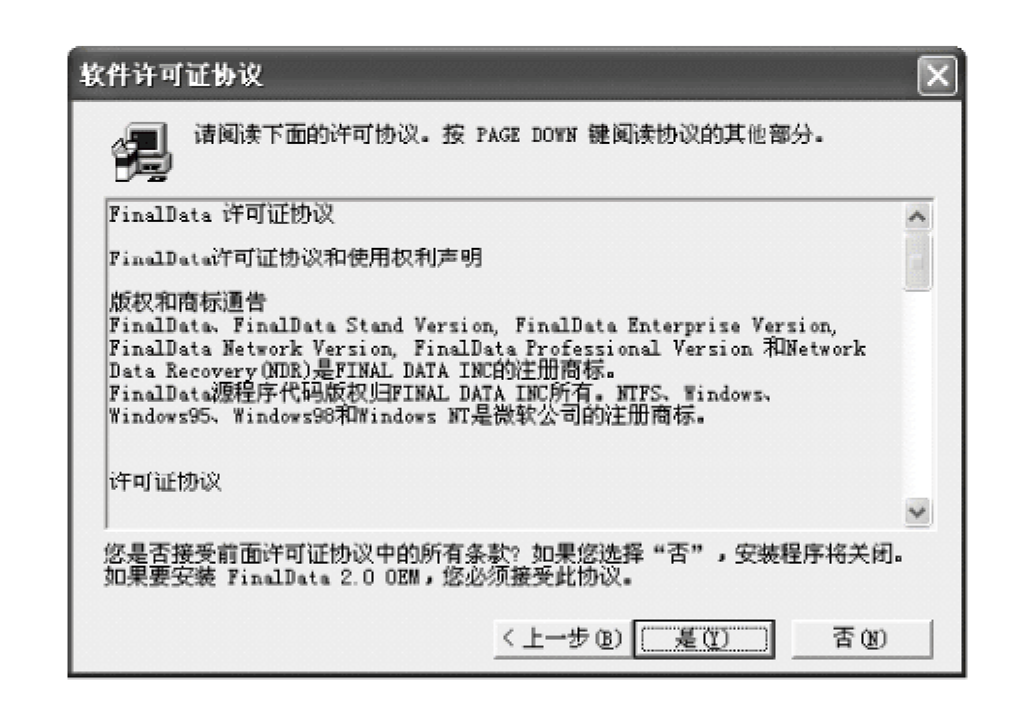


图 13-30 【软件许可证协议】对话框



图 13-31 填写注册用户信息及产品序列号

在【选择目标位置】对话框中，通过单击目标文件夹区域内【浏览】按钮，为 FinalData2.0 选择合适的安装路径（如 e:/），并单击【下一步】按钮，如图 13-32 所示。如果 FinlData2.0 被安装到含有要恢复的数据的驱动器上，数据可能会被永远覆盖从而不能被恢复。因此，需确认要恢复的数据在另外的驱动器上。

选择安装路径后，依次在【选择程序文件夹】和【安装完毕】对话框中，单击【下一步】和【完成】按钮，完成 FinalData2.0 安装。

若要使用 FinalData 2.0 程序进行数据恢复时，可执行【开始】|【程序】|FinalData 2.0 OEM 命令，打开 FinalData 2.0 OEM 窗口。然后，在该窗口的菜单栏中单击【文件】菜单，并执行【打开】命令，如图 13-33 所示。

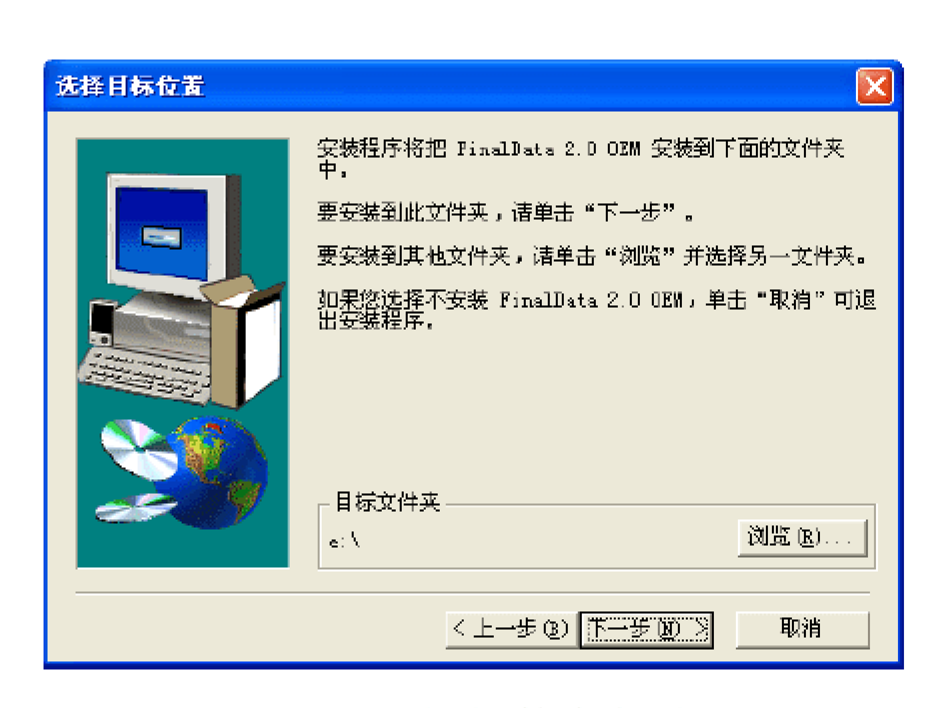


图 13-32　选择软件安装路径

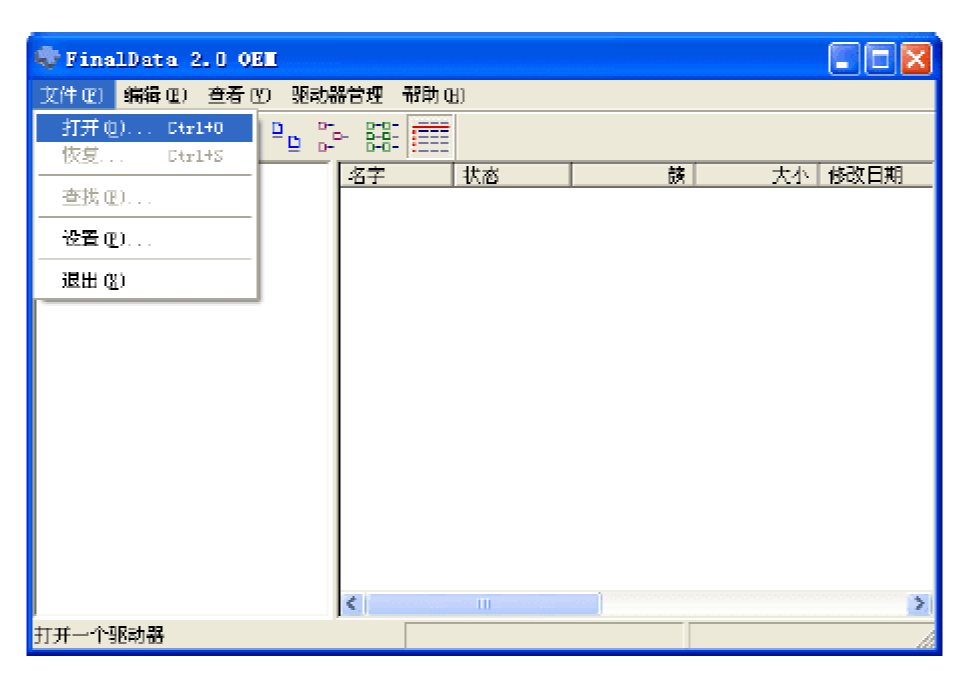


图 13-33　FinalData 2.0 OEM 窗口

在【选择驱动器】对话框中，选择要进行数据恢复的驱动器（如 c:/），然后单击【确定】按钮，如图 13-34 所示。

在【扫描根目录】对话框中，决定是否扫描根目录。如果单击该对话框中【跳过】按钮，那么该程序将不执行对已选择驱动器根目录的扫描。在此，不跳过对根目录的扫描，如图 13-35 所示。



图 13-34　选择驱动器



图 13-35　执行驱动器根目录扫描

在【选择查找的扇区范围】对话框中，可选取已选择的驱动器（c:/）的扫描方式。如果选取完整扫描方式，将会对整个驱动器数据进行查找；如果选择开始扫描方式，则可根据用户设置的查找空间对驱动器的部分扇区进行查找，默认可扫描的最大空间为 2000MB。在此，单击【快速扫描】按钮，如图 13-36 所示。

执行扫描操作后，将在 FinalData 2.0 OEM 窗口中，显示出驱动器内所有的根目录文件、删除的目录和文件、丢失的目录和文件、最近删除的文件及找到的文件等信息。

若要进行数据的恢复，可在该窗口左侧单击要恢复的数据属性（如删除的目录），从右侧数据列表区域选择要恢复的数据（全部或部分），然后单击【文件】菜单，并执行【恢复】命令，如图 13-37 所示。

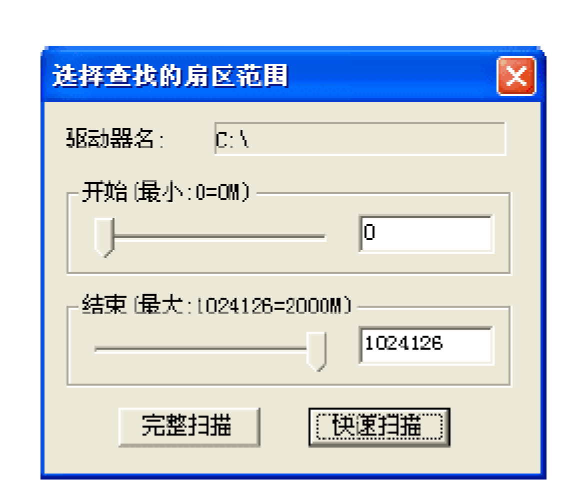


图 13-36　进行快速扫描

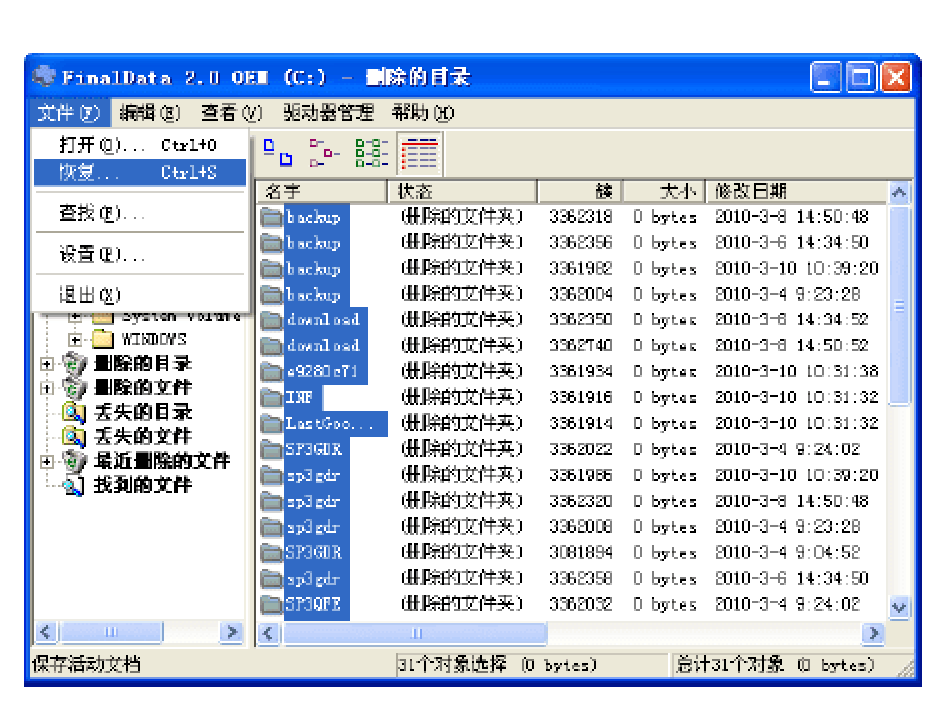


图 13-37　进行数据恢复

在【选择目录保存】对话框中，选择恢复数据的保存位置。可通过单击该窗口左侧驱动器列表中某驱动器（如 E:\），还可通过单击【目录】文本框后方的浏览图标，选择保存位置。确认无误后，单击【保存】按钮，如图 13-38 所示。

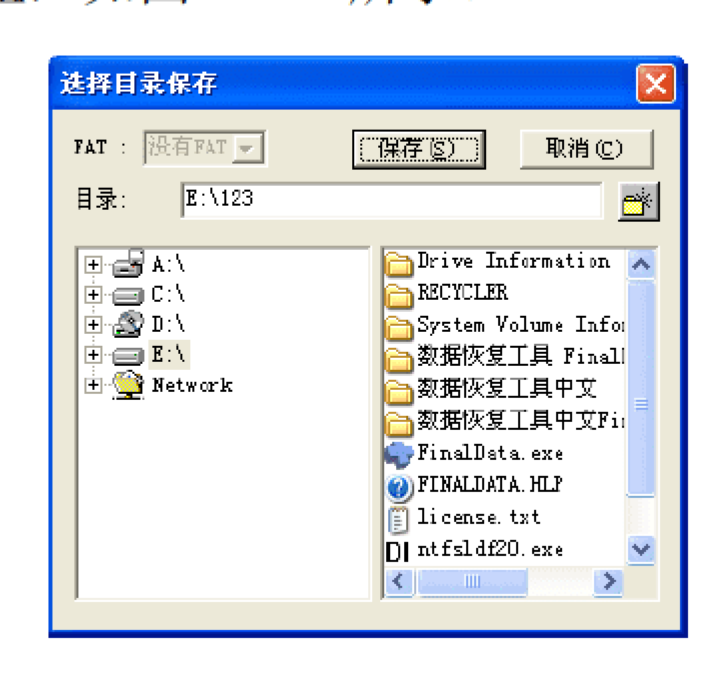


图 13-38　保存恢复数据

13.5.2　EasyRecovery

EasyRecovery 是世界著名数据恢复公司 Ontrack 的技术杰作。其 Professioanl（专业）版是包括了磁盘诊断、数据恢复、文件修复、E-mail 修复 4 大类 19 个项目的各种数据文件修复和磁盘诊断方案。

其支持的数据恢复方案包括如下几种。

- ❑ **高级恢复**　使用高级选项自定义数据恢复。
- ❑ **删除恢复**　查找并恢复已删除的文件。
- ❑ **格式化恢复**　从格式化过的卷中恢复文件。
- ❑ **Raw 恢复**　忽略任何文件系统信息进行恢复。
- ❑ **继续恢复**　继续一个保存的数据恢复进度。
- ❑ **紧急启动盘**　创建自引导紧急启动盘。

其支持的磁盘诊断模式包括如下几种。

- ❑ **驱动器测试**　测试驱动器以寻找潜在的硬件问题。
- ❑ **SMART 测试**　监视并报告潜在的磁盘驱动器问题。
- ❑ **空间管理器**　磁盘驱动器空间情况的详细信息。
- ❑ **跳线查看**　查找 IDE/ATA 磁盘驱动器的跳线设置。
- ❑ **分区测试**　分析现有的文件系统结构。
- ❑ **数据顾问**　创建自引导诊断工具。

若启动 FinalData2.0 安装程序，可双击下载的安装程序“easyrecovery-setup.exe”，然后在【欢迎使用“EasyRecovery Prov6.12.02”安装向导】对话框中单击【下一步】按钮。当出现【选择组件】窗口时，禁用【设置绿色导航站首页】复选框，并单击【是】按钮，如图 13-39 所示。

进行安装组件设置后，需要在【选择安装位置】窗口中，选择 EasyRecovery 的安装路径（E:\Easyrecovery\ Easyrecovery Pro）。可通过单击目录文件夹区域内【浏览】按钮，或直接输入方式进行，然后单击【安装】按钮，如图 13-40 所示。

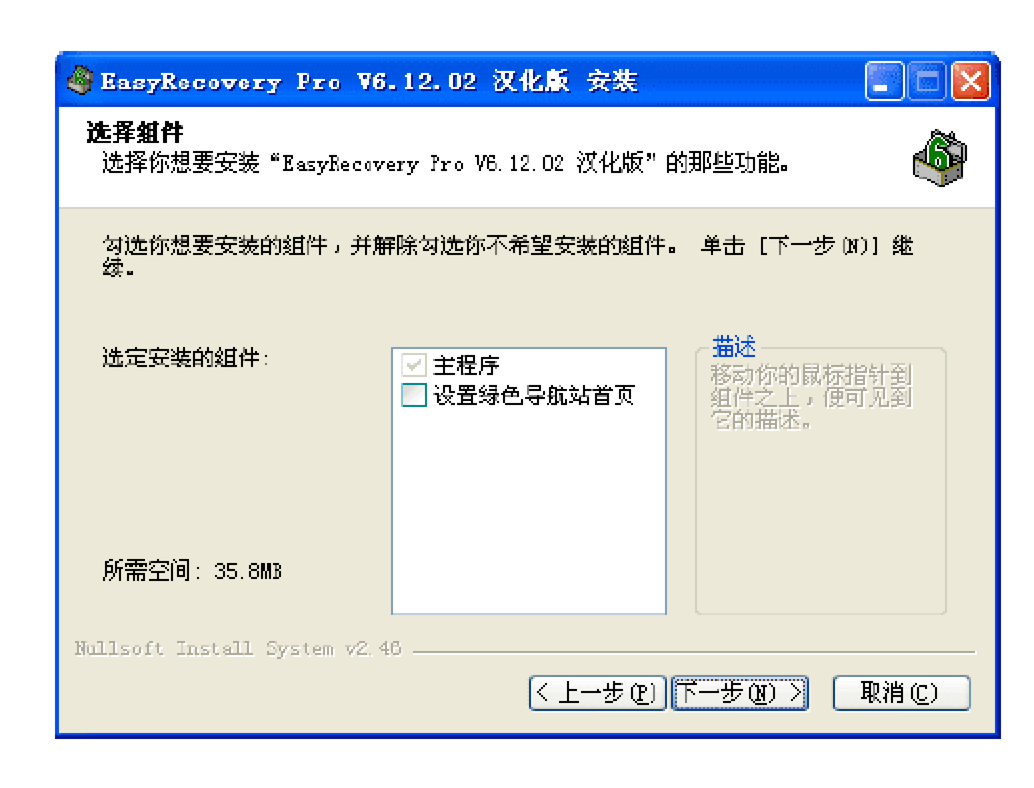


图 13-39　选择安装组件



图 13-40　选择安装位置

选择安装路径后，在【正在完成““EasyRecovery Prov6.12.02”安装向导”】对话框中，单击【完成】按钮，完成 EasyRecovery 的安装。

若要利用 EasyRecovery 程序进行数据恢复或其他操作时，可执行【开始】|【程序】|EasyRecovery Pro 命令，进入 EasyRecovery 主界面。然后在该主界面左侧功能列表中选择【数据恢复】选项卡，将在右侧数据恢复区域内显示提供高级恢复、删除修复、格式化恢复等功能。在此，选择【高级恢复】选项进行数据恢复，如图 13-41 所示。

在【数据恢复高级恢复】窗口中，在左侧驱动器分区列表中，选择恢复数据的分区（E:\），然后单击该界面右下方【高级选项】按钮进行恢复属性设置，如图 13-42 所示。



图 13-41　高级修复

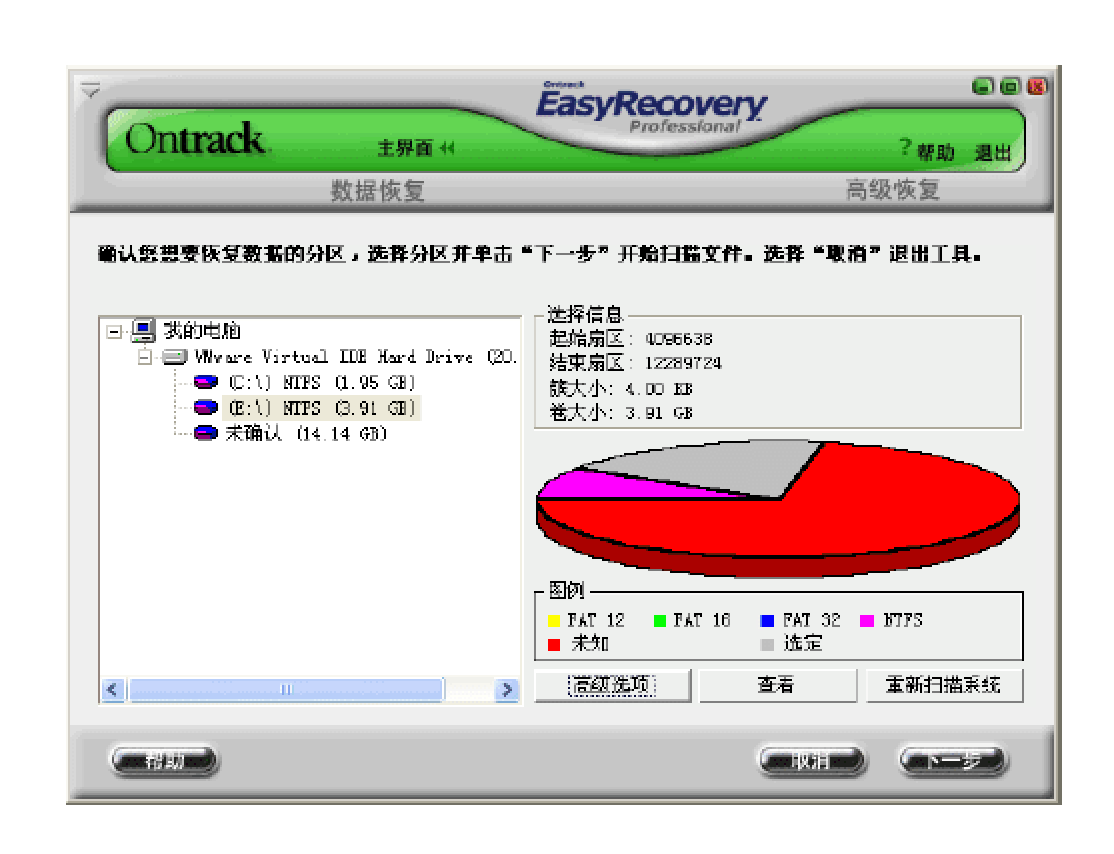


图 13-42 【数据恢复高级恢复】窗口

当出现【高级选项】对话框时，选择【恢复选项】选项卡，可在恢复文件属性区域内启用或禁用文件的属性，然后单击【确定】按钮，如图 13-43 所示。

另外，还可以在 EasyRecovery 主界面左侧功能列表中，选择【文件恢复】选项卡，将在右侧文件恢复区域内显示提供对 Access（数据库）、Excel（电子表格）、PowerPoint（演示文稿）、Word（文档）等这些格式文件的恢复功能。在此，选择【Word 修复】选项进行文件恢复，如图 13-44 所示。

在【文件修复 Word 修复】窗口中，可通过单击【浏览文件】按钮，选择要修复的文件（网络配置与管理.doc），并单击【下一步】按钮，如图 13-45 所示。

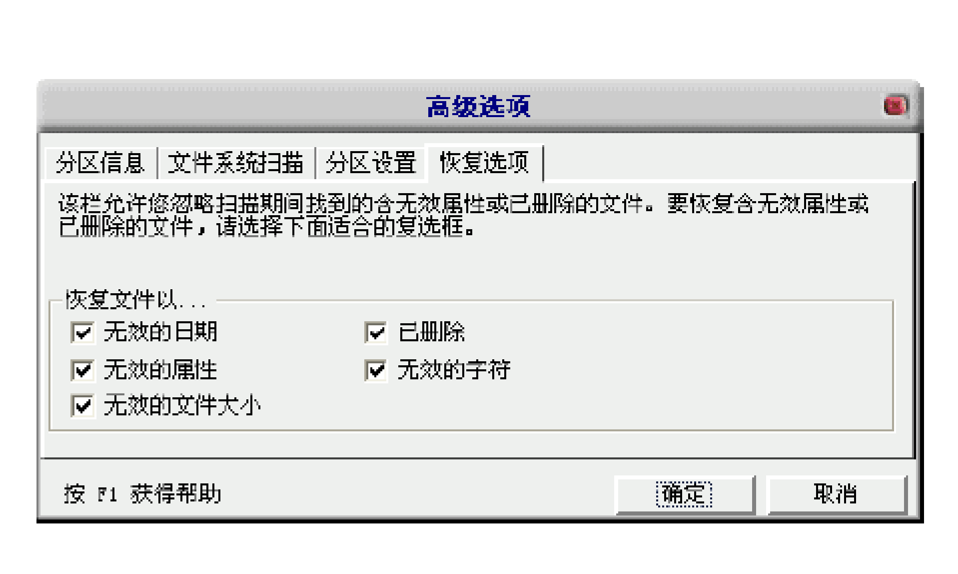



图 13-43　设置恢复文件属性



图 13-44　Word 修复

在【修复报告】窗口中，可查看到已修复文件名称及路径、文件修复完成等信息，如图 13-46 所示。



图 13-45　选择修复文件



图 13-46　修复报告

13.6　操作实例二

13.6.1　操作实例——使用 Windows Server 2003 工具备份/恢复数据

Windows Server 2008 中的 backup 工具是一个可选特性，利用 backup 功能可以有效地帮助用户备份，还原操作系统。

1. 实例目的

- ❑ 备份数据。
- ❑ 删除数据。
- ❑ 恢复数据。

2. 实例步骤

（1）在桌面双击【我的电脑】图标，在打开的窗口中，双击【本地磁盘（D:）】图标，右击任意空白区域，并执行【新建】|【文件夹】命令，并将文件重命名为“slyx”，如图 13-47 所示。

（2）执行【开始】|【程序】|【管理工具】|Windows Server Backup 命令，在弹出的窗口中，选择右侧【操作】窗格中的【一次性备份】选项，如图 13-48 所示。

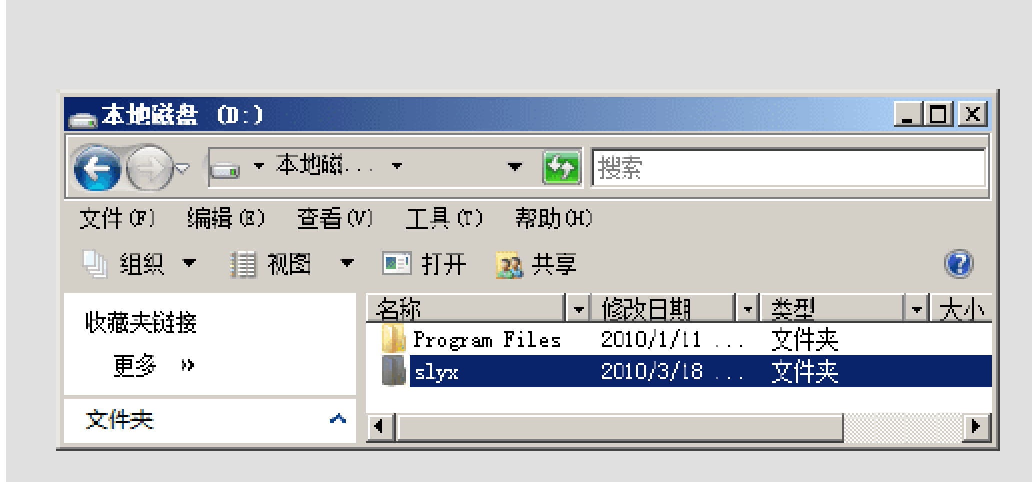


图 13-47　创建文件夹

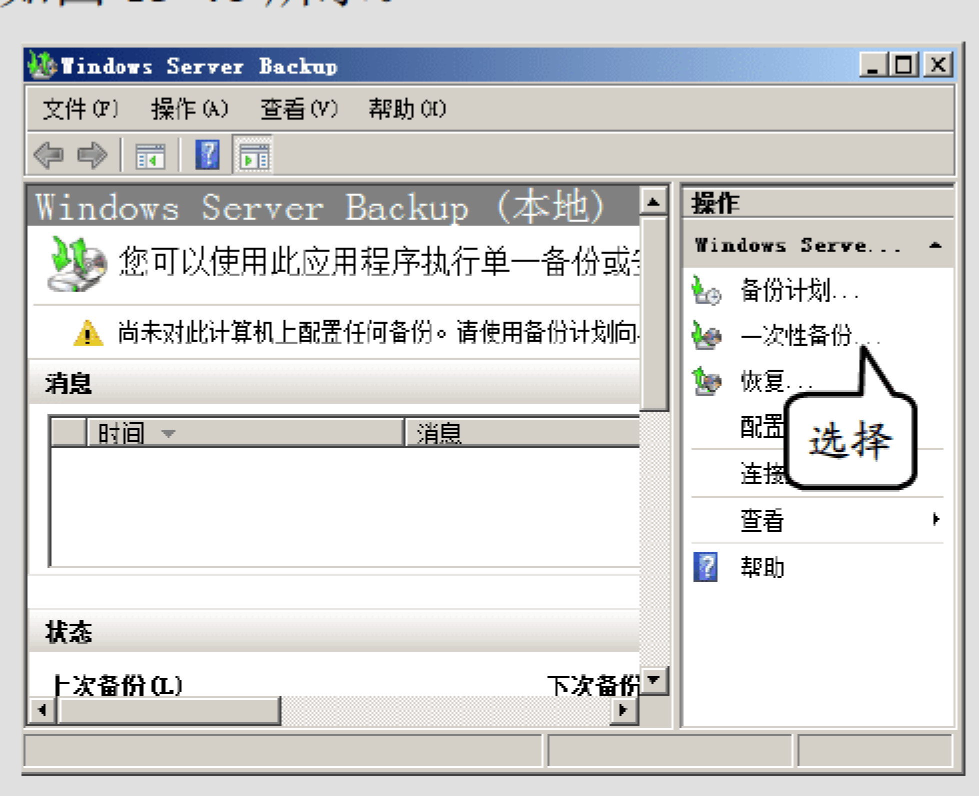


图 13-48　一次性备份

（3）在【备份选项】对话框中，单击【下一步】按钮，如图 13-49 所示。

（4）在【选择备份配置】对话框中，选中【自定义】单选按钮，单击【下一步】按钮，如图 13-50 所示。



图 13-49　选择备份方式

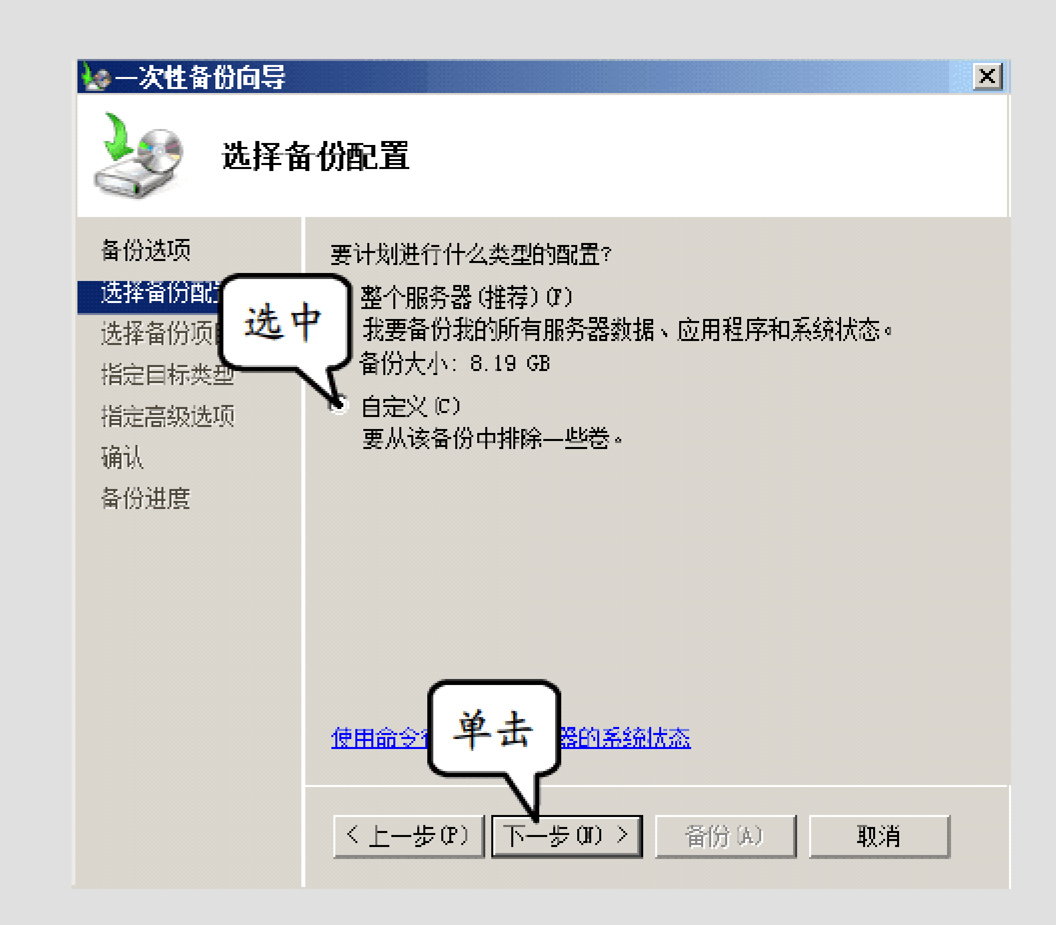


图 13-50　备份配置选项

（5）在弹出的对话框中，选中【本地磁盘（D:）】单选按钮，单击【下一步】按钮，如图 13-51 所示。

（6）在【指定目标类型】对话框中，选中【本地驱动器】单选按钮，并单击【下一步】按钮，如图 13-52 所示。

（7）在弹出的对话框中，选择备份位置，并单击【下一步】按钮，如图 13-53 所示。

（8）在【指定高级选项】对话框中，选中【VSS 完全备份】单选按钮，单击【下一步】

按钮，如图 13-54 所示。

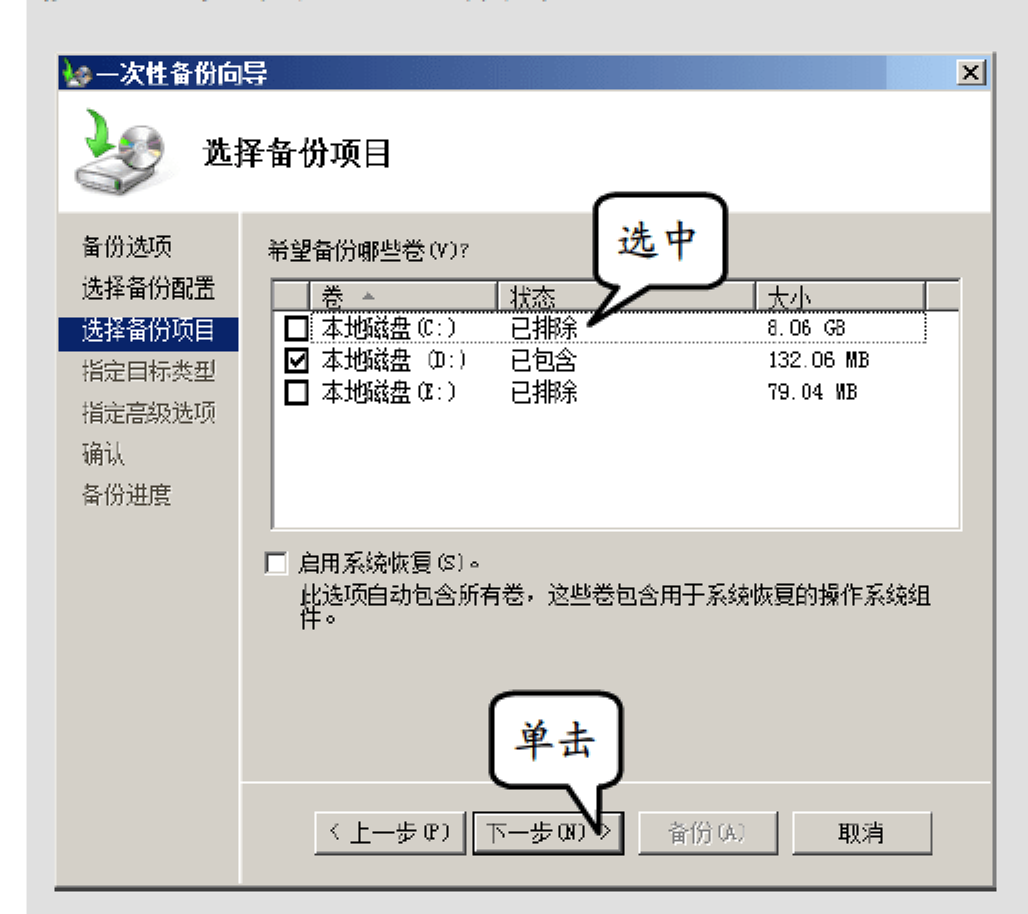


图 13-51　备份 D 盘数据



图 13-52　本地驱动器



图 13-53　备份目标为本地磁盘（E:）

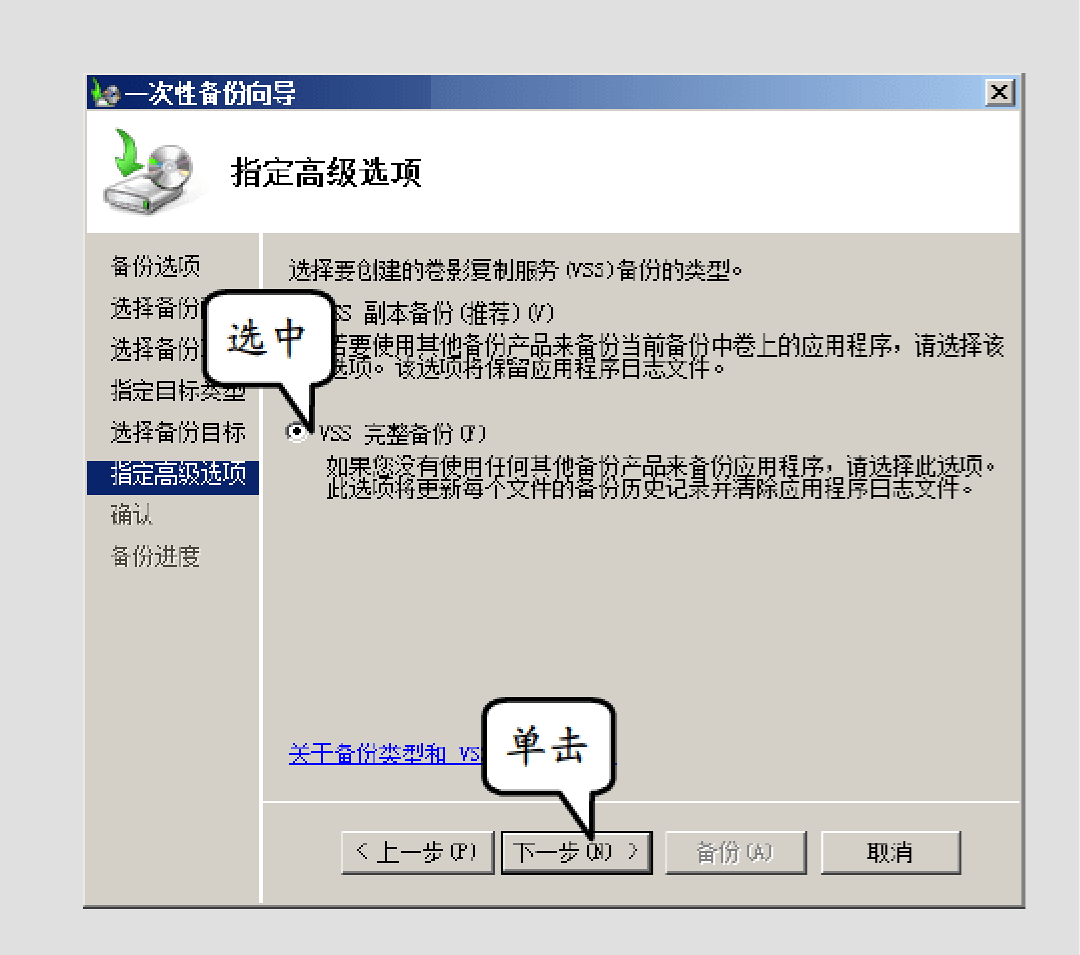


图 13-54　完全备份

（9）在【确认】对话框中，单击【备份】按钮，如图 13-55 所示。

3. 恢复数据

（1）在【本地磁盘（D:)】中，右击 slyx 文件夹，并执行【删除】命令。在 Windows Server Backup 窗口中，选择【恢复】选项，如图 13-56 所示。

（2）在弹出的【入门】对话框，单击【下一步】按钮。在【选择备份日期】对话框中，单击【下一步】按钮，如图 13-57 所示。

（3）在弹出的对话框中，选中【文件和文件夹】单选按钮，并单击【下一步】按钮，如图 13-58 所示。

（4）在【选择要恢复的项目】对话框中，依次展开 WIN-VG2WB2JHS4A 和 slyx 节点，并单击【下一步】按钮，如图 13-59 所示。

（5）在弹出的对话框中的【恢复目标】栏内选中【原始位置】单选按钮，并单击【下一步】按钮，如图 13-60 所示。

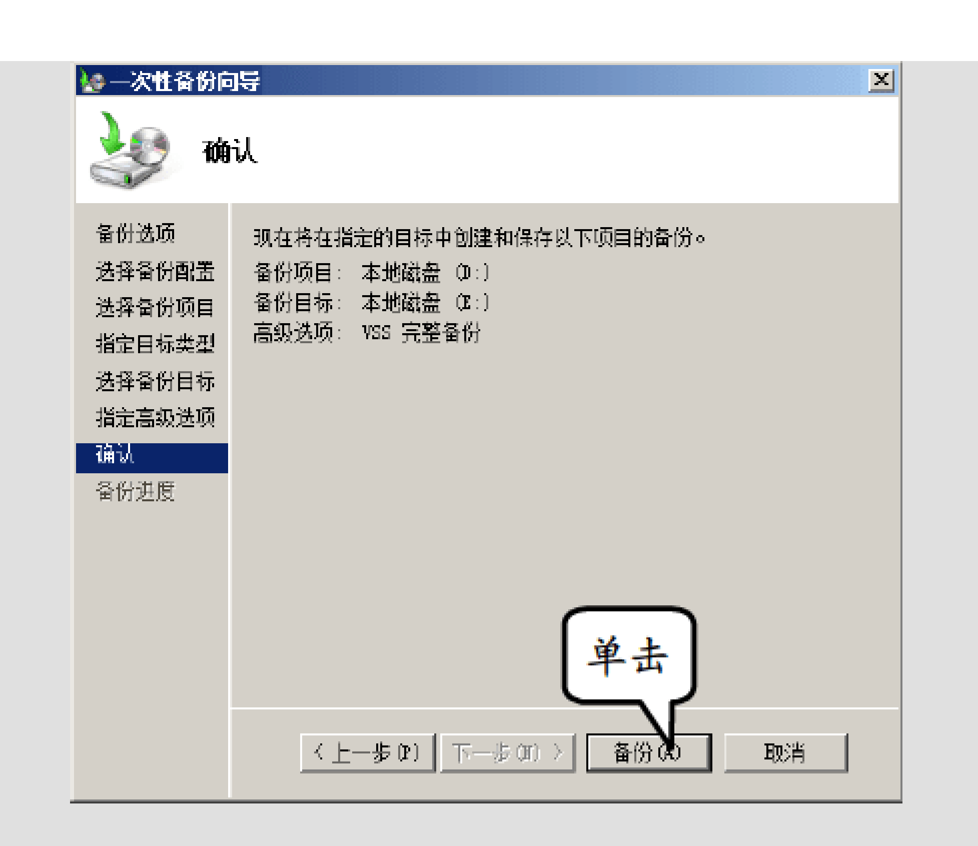


图 13-55　配置结果

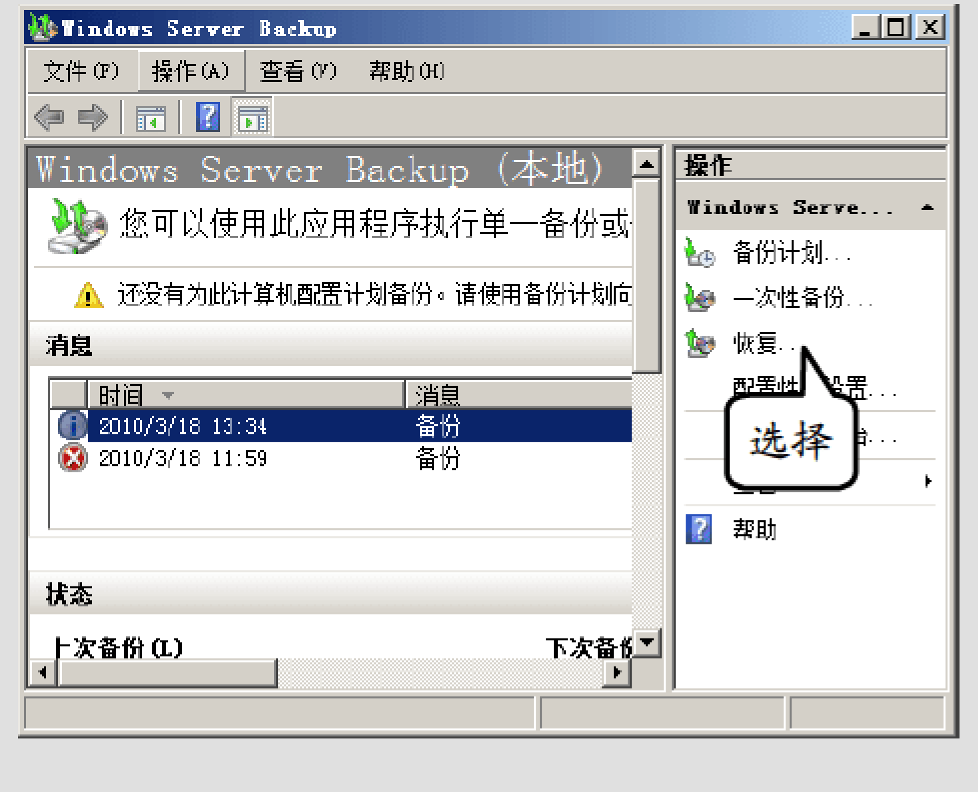


图 13-56　开始恢复



图 13-57　选择备份日期

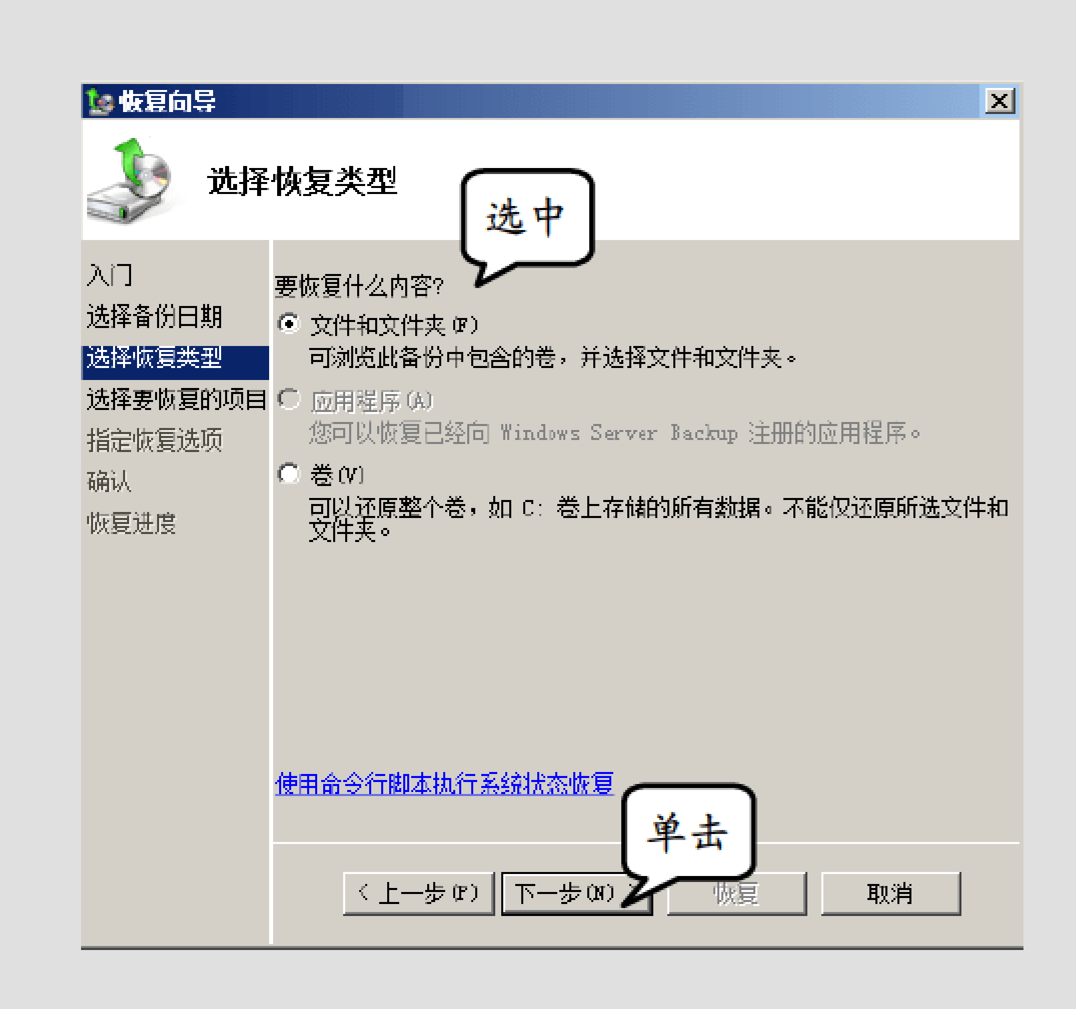


图 13-58　选择恢复类型



图 13-59　选择要恢复的项目

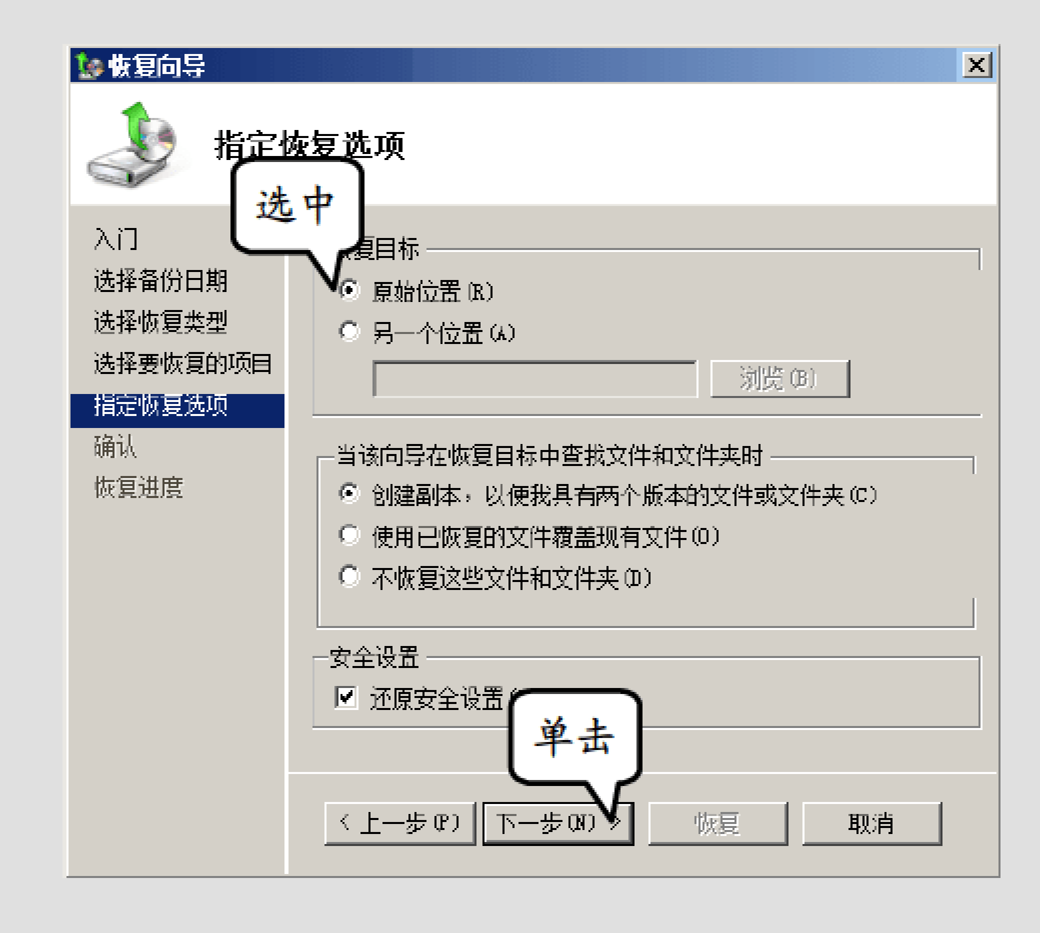


图 13-60　原始位置恢复

（6）在【确认】对话框中，单击【恢复】按钮，恢复完成后，在【本地磁盘（D:)】中，

查看已恢复文件，如图 13-61 所示。

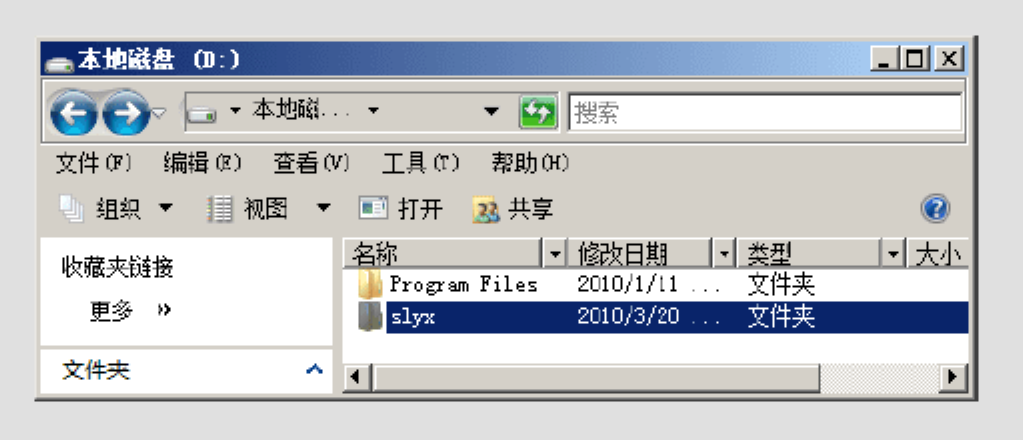


图 13-61　查看恢复文件

13.6.2　操作实例——数据库的备份/恢复

如果服务器数据库发生故障或遭到黑客入侵，会造成大量的数据丢失。这样服务器将会瘫痪，从而导致整个网络瘫痪。因此做好数据库的备份工作就显得很重要。

1. 实例目的

- 备份活动目录数据库。
- 恢复活动目录数据库。

2. 实例步骤

（1）在桌面执行【开始】|【运行】命令，在【运行】对话框中，输入 cmd 命令，并单击【确定】按钮，如图 13-62 所示。

（2）在【命令提示符】窗口中，输入 wbadmin get disks 命令，并按回车键，如图 13-63 所示。

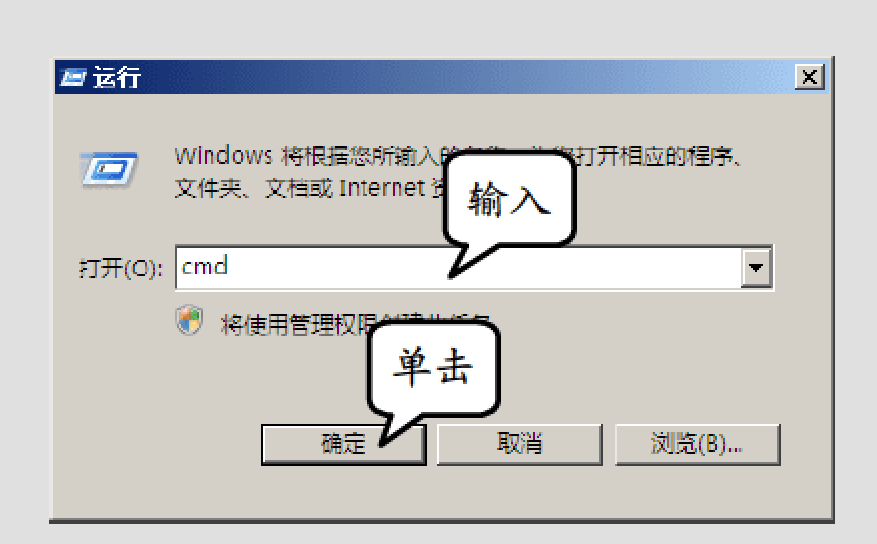


图 13-62　【运行】对话框



图 13-63　查看联机的磁盘

（3）输入 wbadnim start backup –backuptarget：d：-includes：c：（将磁盘 c 备份到磁盘 d）命令，并按回车键，然后，根据提示输入 y（确定备份）命令并按回车键，如图 13-64 所示。

（4）在【命令提示符】窗口中输入 wbadmin get versions 命令，并按回车键，如图 13-65 所示。

3. 备份数据库

（1）重新启动计算机，在进入 Windows Server 2008 的初始窗口前按 F8 键，在高级启动选项菜单界面，使用方向键移动光标到【目录服务还原模式】选项，并按回车键，如图 13-66

所示。

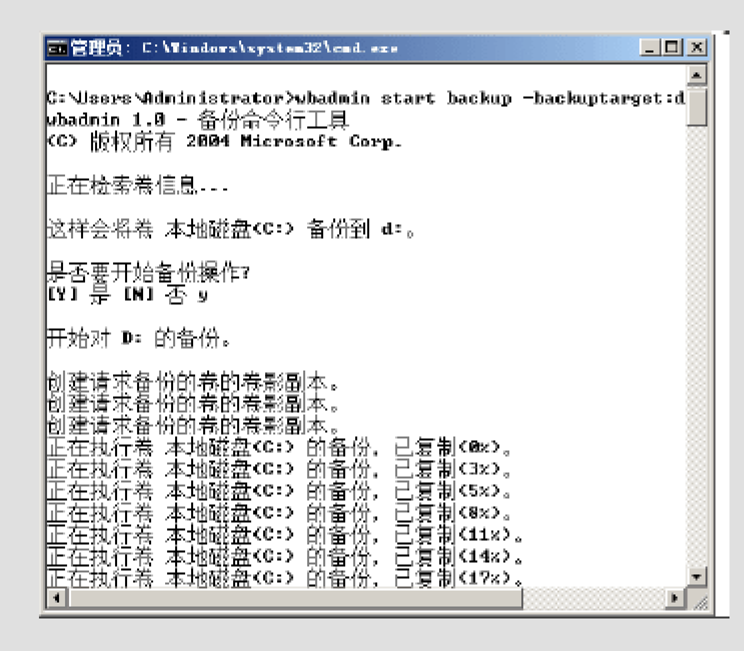


图 13-64　执行备份命令

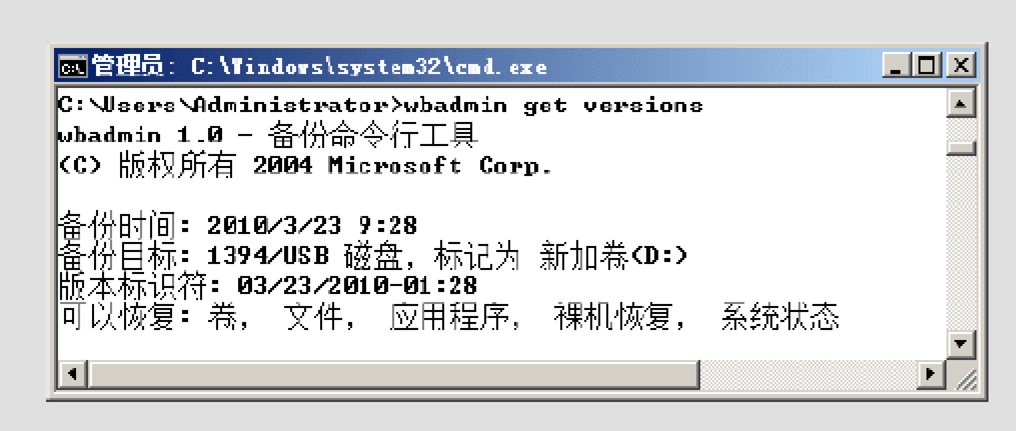


图 13-65　备份状态信息

（2）在桌面执行【开始】|【运行】命令，在【运行】对话框中输入 cmd 命令，并单击【确定】按钮，在【命令提示符】窗口内输入 wbadmin get versions 命令，按回车键，如图 13-67 所示。

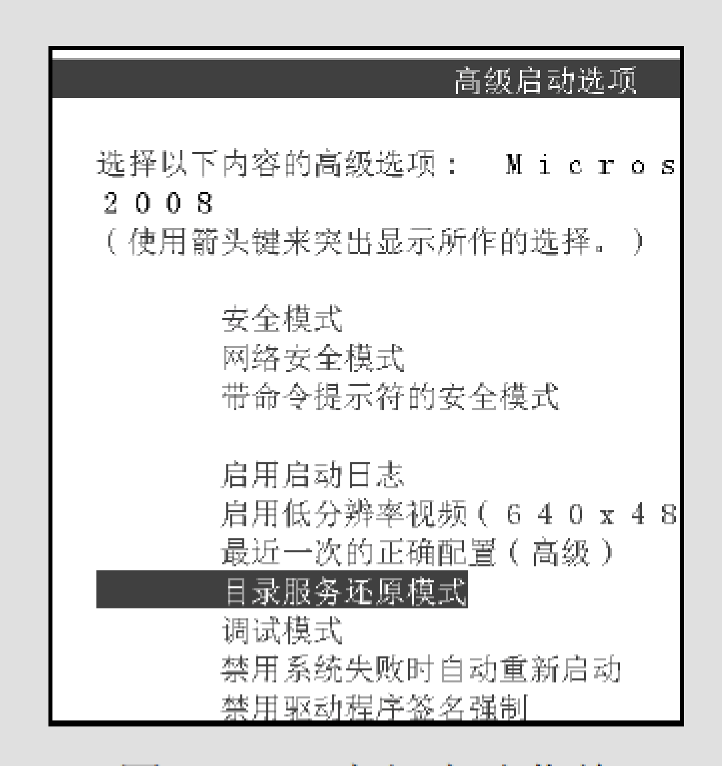


图 13-66　高级启动菜单

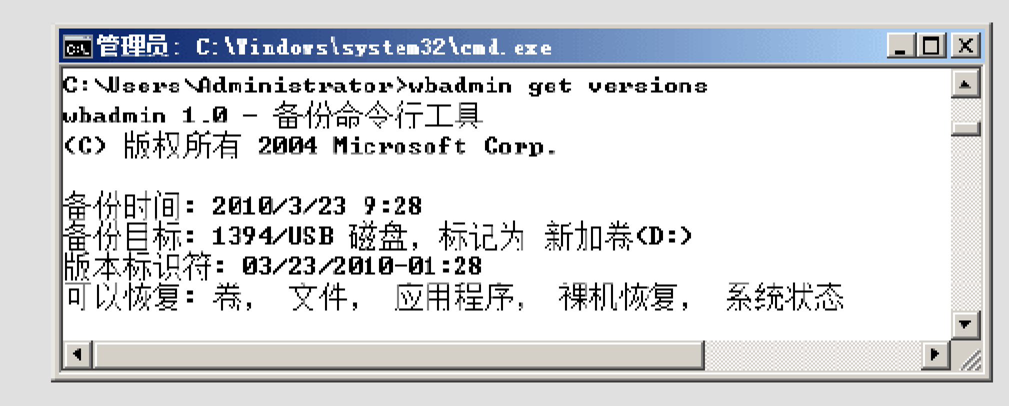


图 13-67　查看备份表示符

（3）输入 wbadmin start systemstaterecovery –versions：03/23/2010-01：28（恢复 2010 年 3 月 3 日的数据）命令，并按回车键，根据提示输入 y（确定开始）命令并按回车键，如图 13-68 所示。

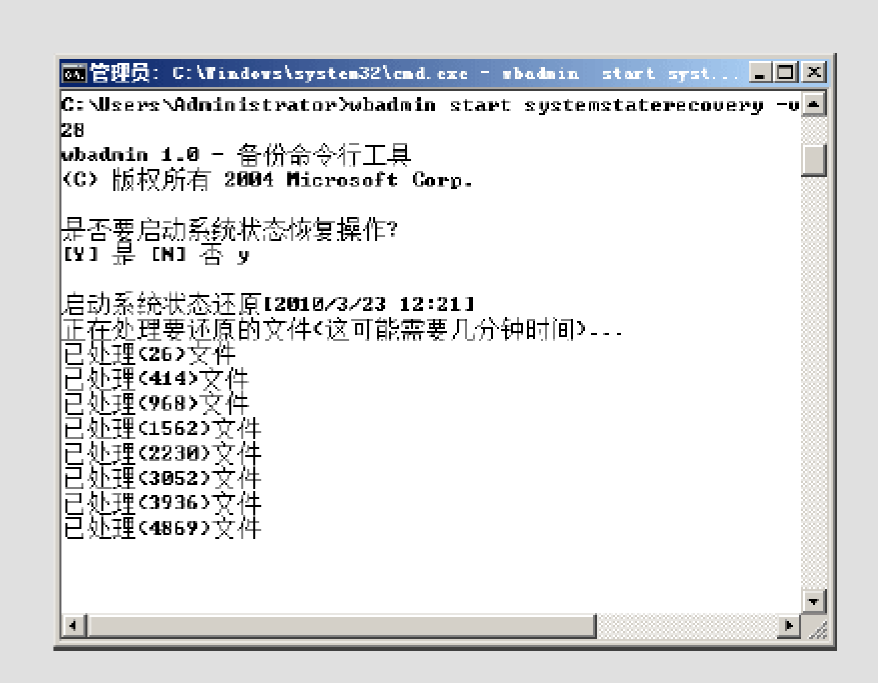


图 13-68　恢复数据



以上进行的是非授权恢复：所有未经授权恢复的数据，都将在活动目录复制系统中出现，虽然数据是旧的，但是不会复制到其他服务器中。